IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

- - - - - - - - - - - - - - - - - - - - - - - - - -

| | | |
|---|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>GERALD ANDREW DARBY,<br><br>Defendant. | ) | CRIMINAL CASE NO.<br>2:16cr00036 |
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>HUNTER VAUGHAN EURE,<br><br>Defendant. | ) | CRIMINAL CASE NO.<br>2:16cr00043 |

- - - - - - - - - - - - - - - - - - - - - - - - - -

TRANSCRIPT OF PROCEEDINGS
Norfolk, Virginia
July 5, 2016

BEFORE: THE HONORABLE ROBERT G. DOUMAR,
United States District Judge

APPEARANCES:

UNITED STATES ATTORNEY'S OFFICE
By: Elizabeth M. Yusi
Leslie W. Fisher
Assistant United States Attorneys
Counsel for the United States

FEDERAL PUBLIC DEFENDER'S OFFICE
By: Andrew W. Grindrod
Richard J. Colgan
Rodolfo Cejas, II
Assistant Federal Public Defenders
Counsel for the Defendants

# INDEX

# EXHIBITS

(The proceedings commenced at 2:30 p.m., as follows:)

THE CLERK: Criminal Case No. 2:16cr36, United States of America v. Gerald Andrew Darby.

Ms. Fisher, Ms. Yusi, are you ready to proceed on behalf of the United States?

MS. YUSI: We are.

Good afternoon, Your Honor.

THE CLERK: Mr. Cejas, are you ready to proceed on behalf of the defendant?

MR. CEJAS: Yes, we are.

THE CLERK: And in Case No. 2:16cr43, the United States v. Hunter Vaughan Eure, Ms. Yusi, Ms. Fisher, are you ready to proceed?

MS. YUSI: We are, Your Honor.

THE CLERK: And Mr. Grindrod and Mr. Colgan, are you ready to proceed on behalf of the defendant?

MR. GRINDROD: We are.

Good afternoon, Your Honor.

THE COURT: I would like to take up the motion to suppress by Mr. Eure first, which we haven't ruled upon, and then we will deal with the motions to compel jointly so that we just don't reiterate everything and we won't have two.

So let's take up Mr. Eure's motion to suppress at this time. And I assume, Mr. Grindrod, you're arguing that.

MR. GRINDROD: I am, Your Honor, and we also have evidence, if we could, Your Honor.

THE COURT: All right. I'll be glad to hear from you. It's your motion.

MS. YUSI: May I have a moment, Your Honor?

THE COURT: Sure.

(There was a pause in the proceedings.)

THE COURT: All right. Go ahead.

MR. GRINDROD: Your Honor, the defense calls Dr. Christopher Soghoian to the stand.

(The clerk administered the oath.)

MR. GRINDROD: And, Your Honor, Dr. Soghoian is going to be testifying as to matters that relate both to suppression and the motions to compel. I can separate them and recall him later, or I can ask all the questions at once, Your Honor.

THE COURT: Well, since we're having a joint hearing, my suggestion is he's going to testify in both, and maybe that would save us some time, assuming counsel for Mr. Darby would agree.

MR. CEJAS: Yes, sir, that's fine.

THE COURT: Thank you, Mr. Cejas.

MR. GRINDROD: May I inquire, Your Honor?

THE COURT: Yes, go ahead.

CHRISTOPHER SOGHOIAN, Ph.D., called as a witness, having been first duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. GRINDROD:

Q. Good afternoon, sir. Could you please introduce yourself to the Court.

A. My name is Christopher Soghoian.

Q. And why are you here today, sir?

A. I volunteered in my personal capacity as an expert so that the defense and so that the Court can have a better understanding of the technology used by the FBI in this case.

Q. Okay. I want to talk to you about a little bit of background, about your experience and qualifications. Could you tell us a little bit about your educational background?

A. Sure. I have a Bachelor's degree in computer science from James Madison University, I have a Master's degree in security informatics from the Johns Hopkins University, and I have a Ph.D. in informatics from Indiana University.

Q. Can you tell us a little bit about your experience working in these fields?

A. Sure. So in my job at the ACLU and before that at the Federal Trade Commission I am a computer scientist who explains technology to lawyers.

My Ph.D. was focused in the analysis of surveillance techniques used by the U.S. Government, and specifically I help lawyers understand how the government engages in high tech surveillance. So at the ACLU, where I'm employed, I work with the lawyers who litigate Fourth Amendment cases, and I make sure that they understand the technology and that they are accurately describing it in the cases in which they're engaged.

Q. And what is your position at the ACLU?

A. I'm employed as the ACLU's principal technologist in our Speech Privacy and Technology Project.

Q. Do you currently hold any other position?

A. I'm also a visiting fellow at the Information Society Project at Yale Law School.

Q. And have you received any awards or honors in your field?

A. I've received a couple of awards. Politico magazine last year named me one of the top 50 people affecting policy in the United States. That's the one I can remember off the top of my head.

Q. That's fine. Have any courts cited your work?

A. My academic research on surveillance has been cited by a few federal courts, including the Ninth Circuit Court of Appeals, and by the State Supreme Courts of Massachusetts and New Jersey.

THE COURT: Where was this academic research? You just said your academic research.

THE WITNESS: Yeah. I have law review articles that have been published in the Harvard Journal of Law and

Technology, the Berkley Journal of Law and Technology, and the Yale Journal of Law and Technology, and so that research has been cited by those courts.

BY MR. GRINDROD:

Q. And has any of your work focused specifically on remote technology or malware?

A. I've been researching NITs, the network investigative techniques, for about five years, and in the course of that research I have learned quite a bit about the technology, I've interviewed people who have worked in the teams at the FBI that deliver this technology, and I've analyzed some of the code that the FBI has used.

Q. And have you done -- we've talked a lot about the training you've received. Have you given any training or spoken on these topics?

A. Sure. So I've been invited to several training events organized by the Federal Judicial Center, so I've given training to judges, both District Court Judges, Magistrate, and even Circuit Court Appellate Judges, about surveillance technology, including the use of NITs.

Q. Have you offered testimony before any legislative bodies or rule-making committees about these topics?

A. Yeah. I've testified before, I think, three different state legislative bodies in the United States, the European Parliament, and I also testified before the rules committee that put out the changes to Rule 41 regarding the use of these technologies.

Q. Okay. And now I want to talk to you specifically about your preparation for your testimony in this case.

First of all, do you have any background knowledge on NITs or network investigative techniques?

A. So, as I said, I've been researching NITs for about five years. I've testified in two cases, two prior cases where NITs have been used, as a volunteer, an unpaid volunteer, for the defense in those cases. I've reviewed numerous case filings. I've reviewed transcripts from Special Agent Alfin and others.

And then, under protective order in various cases, I've looked at some of the code and some of the two-way network recordings as well.

Q. Okay. Have you looked at the code and the PCAP data that was produced in Mr. Eure's case?

A. I have.

Q. You said you're here in your personal capacity. Is that right?

A. Yes.

Q. Are you being paid for your services in this case by the defense?

A. My flight was paid for, and I think my taxi fees will be reimbursed, but I'm not receiving any kind of honorarium or consulting fee, no.

Q. Okay. So why is it that you volunteer in cases like this?

MS. YUSI: I object, Your Honor. What's the relevance of this?

THE COURT: Objection sustained.

BY MR. GRINDROD:

Q. I want to talk to you about --

A. I'm sorry. Can I get a glass of water, too? Is that possible?

MR. GRINDROD: Yes.

(There was a pause in the proceedings.)

BY MR. GRINDROD:

Q. Are you familiar -- I want to talk to you about a couple issues having to do with suppression. So, first, are you familiar with the government's argument that the NIT that was deployed in this case --

THE COURT: Stop. You're getting into the case itself so, consequently, are you finished with the voir dire of this witness's qualifications?

MR. GRINDROD: Yes, Your Honor.

THE COURT: Ms. Yusi, do you have any questions on voir dire?

MS. YUSI: I don't, Your Honor, but I also don't know what he's being offered for as an expert in.

THE COURT: Well, I'm sure he'll tell us.

MS. YUSI: Okay.

THE COURT: Go ahead, Mr. Grindrod.

MR. GRINDROD: Thank you, Judge.

BY MR. GRINDROD:

Q. Are you familiar with the argument that's been raised by the government in this case and related cases that the NIT that was deployed in this case worked like a tracking device?

A. I am familiar with that theory.

Q. And just so we're on the same page, that argument goes, basically, that a Playpen user entered the government server hosting Playpen, which --

MS. YUSI: Objection, Your Honor. He's testifying. If he wants to ask a direct question...

THE COURT: Objection sustained.

BY MR. GRINDROD:

Q. Can you tell me what your understanding of the government's argument is with respect to this tracking device?

THE COURT: It's not the government's argument, it's what his understanding of what is utilized in this case is. Don't let's talk about somebody else's argument.

He's not an expert on the argument, okay? He's an expert on the use of the Internet. He can also describe all of his uses. He can tell me what a NIT is, but he's not going to tell me whether the argument of the government is appropriate or inappropriate in any way. He can discuss all he wants about any factual matter or his opinions, but not his opinions of somebody else's case.

Do we understand one another, sir?

MR. GRINDROD: Yes, Your Honor.

THE COURT: Okay.

BY MR. GRINDROD:

Q. Can you tell me from a technological perspective where the NIT is installed, the location, the physical location?

A. So the computers that were visiting the Playpen Web site ultimately had to contact the government server, which was located somewhere in Northern Virginia. Although the code, the computer instructions for the NIT, was hosted on the government's computer, it didn't activate. It didn't do anything until it was transmitted all the way over the Internet to the receiving parties, to the computers that were visiting the Web site, and then ultimately ran on those individual computers.

THE COURT: You lost me, so let's go back.

THE WITNESS: Let's try again. Okay.

So there were a number of people who visited the Playpen Web site. They connected to the Playpen Web site using this technology called Tor, but ultimately there was a Web browser, like Firefox or Internet Explorer or Chrome, and then they used their Web browser to visit a Web site.

The NIT, the network investigative technique, was delivered to the computers of the people who were visiting this Web site, and the network investigative technique --

THE COURT: Well, what you have to do is to say what visited the network site, not "the NIT visited."

"The NIT visited" is too broad a concept. That's investigative techniques. So what we want to deal with are the specifics, and that's what I've got to hear. Otherwise, you just become another attorney for the defendant. Don't become the attorney, just become the expert, okay?

THE WITNESS: Yes, Your Honor.

And, to be clear, I'm not an attorney. I didn't go to law school.

THE COURT: Well, by the time you finished explaining your background, you probably know more than most attorneys who are dealing with this subject.

THE WITNESS: I appreciate that, sir.

THE COURT: So let's get on with what we're doing here.

First, one thing I want to find out about qualifications -- I might as well do it now that I've interrupted you -- is are you paid a salary by the ACLU?

THE WITNESS: I am paid a salary, sir, but I'm taking a vacation day to come here.

THE COURT: You're taking a vacation?

THE WITNESS: A one-day vacation.

THE COURT: Do they give you vacation days?

THE WITNESS: I receive vacation days at the ACLU. Not as many as I would like.

THE COURT: So what I'm getting at is you're not losing any money, as such.

THE WITNESS: No, I'm not.

THE COURT: And when you say you're an unpaid volunteer, you are a volunteer here, but I assume it's with the understanding of the ACLU.

THE WITNESS: I have to ask my boss for permission to take time off, yes.

THE COURT: I figured that. So I just want to know where we are and what we are dealing with. So, consequently, you can go on from there, but let's stick to the facts and your expertise, okay?

MR. GRINDROD: Thank you, Your Honor.

THE WITNESS: Sir, if I might add one more thing, I just want to clarify.

I asked to come here from my -- I asked for permission from my employer, as opposed to being told by my employer, "Hey, Chris, take a day off and go down to Norfolk."

THE COURT: Oh, I understand that.

BY MR. GRINDROD:

Q. Okay, Dr. Soghoian. So I think you were starting to explain kind of the technology -- how the NIT works from a technological standpoint. So if you could tell us where -- first of all, what is -- Judge Doumar just asked this.

So what is the NIT? When we're talking about the NIT and we talk about code associated with it, can you just tell us what that is?

A. The NIT is a specially made computer program that is designed to surreptitiously collect information from one or more person's computers, collect that information, and transmit it back to the government.

Q. Okay. So even kind of more specifically than that, when we talk about the NIT being computer code, what is that? What is computer code?

A. So if you think of the blueprints for a building versus the building itself, human beings write code, and computer scientists who know how to write computer programs, they create code by writing it in a special language. But it's still human readable, readable by humans who understand computers, and then the computer turns it into a special language that is easier for the computer to understand. So that's called computer code.

Q. Okay.

A. And, essentially, they're a series of instructions that tell the computer, do this, do that, do this other thing.

Q. And computer code, is that something that only exists in the government surveillance context, or does computer code exist --

A. No, every single electronic device that we have in our lives, from a cell phone to an ATM machine to an airplane, has computer code in it now.

Q. So the question I asked you a little while ago was trying to understand where the computer code that we're talking about in this case, the NIT, where that actually was deployed, where it worked. So can you explain, just from a technological perspective, focusing on the facts, where that happened?

A. Sure. The computer code, the NIT code in this case, would have been downloaded from a server run by the FBI in Northern Virginia, downloaded to the computers of the individual people visiting the Playpen site, including the alleged defendants in this case. But it would not have run, the code would not have done anything, until it reached their computers and ran on their computers.

You could think of the code as being inert. It didn't have the power to do anything until it ran on the computers of the individual defendants.

Q. And was the -- until the code was installed on our client's computer, would there have been -- did it serve any functional purpose for anyone who would have been using the code?

A. The code would never have run on anyone's computers but the defendant's computer, you know, unless an FBI agent ran it in the lab to test it out. But when it was sitting on the government's Web server, its Web site, waiting to be downloaded it would be sitting dormant. It wasn't doing anything. It wasn't hurting anyone or helping anyone. It was just sitting there like an unopened piece of mail, and someone had to go and get it, bring it back, and it was only then, once it was executed on the defendant's computer, that it would come to life and that it would have the resources to then run. And with those resources with a computer that had power and had the ability to think, the processing capability, then the NIT could come to life and perform the instructions that it had been programmed to do; in this case, to collect various forms of information from the computer that it was operating on and then to call home to the government server with those bits of information.

Q. In any technological sense, did the user of an activating computer visit the FBI's server?

A. The individual users of the Playpen site certainly communicated with the government's server. They requested Web pages, and the Web pages were then returned to those individuals. Those individuals never left their homes. They didn't get in their car and drive across country or up --

THE COURT: So the code had nothing to do, then, with the requested Web pages of the --

THE WITNESS: The Web pages were viewed by the individual users --

THE COURT: I'm asking once it was sent to the government -- to Playpen, we'll call it, and you're familiar with it. The code had nothing to do with that.

THE WITNESS: The code --

THE COURT: The code is merely an investigatory matter, correct?

THE WITNESS: The NIT code was delivered to the visitors of the site at the same time as they were visiting the Web page.

THE COURT: I understand, but the site itself would know what was requested of it, correct?

THE WITNESS: When you say "the site," I mean --

THE COURT: Playpen.

THE WITNESS: I understand Playpen, but Playpen was a Web site, it wasn't a human, so when you say did the site know do you mean the people operating the Web site, did they know? Because they were FBI agents, they definitely knew what was being delivered.

THE COURT: Once the Web site gets something, does the Web site know it got it?

THE WITNESS: The --

THE COURT: Does it record?

THE WITNESS: I think I know what you're asking.

When the NIT called home it did not call home to the Playpen site. The NIT was delivered to people who were visiting Playpen; that when the NIT called home it called home to a different computer run by the FBI.

THE COURT: All I'm asking you is Playpen. It receives something, correct?

THE WITNESS: The -- when the user visits the Playpen site, they request a Web page. They get that Web page back, and that response would have included -- I'm trying to figure out how to explain this in terms that are easy to --

THE COURT: Playpen responds to whatever the request is, and all I'm saying is there's a record of that response, correct?

THE WITNESS: When you say -- you mean a permanent record?

THE COURT: I don't know if it's permanent or anything. I assume Playpen has some knowledge of what it sends.

THE WITNESS: That would really depend on how the FBI configured the Playpen site.

THE COURT: I'm not worried about the FBI, I'm worried about Playpen, the site itself.

Once the FBI runs it, it's just running a site, correct?

THE WITNESS: Again, that really depends on how the FBI is running the site. If I can use an analogy, Your Honor, the PACER Web site that this court runs that people can download documents from, there may be records that are kept of every document I download from PACER; there may not be. It really depends on how the administrators of this courthouse configure the Web site to operate.

I don't know whether the FBI, when they were operating the Playpen site -- whether they recorded every single thing that the Web site sent or nothing.

THE COURT: So the FBI has the site, correct?

THE WITNESS: The FBI was running the Playpen site, yes, sir.

THE COURT: And they don't know what's happening on the site. Is that your testimony?

THE WITNESS: No, Your Honor.

THE COURT: Oh, so they know what's happening on the site.

THE WITNESS: Your Honor, I'm saying I don't know what the FBI knew because I don't know how the FBI configured Playpen. And the Playpen site is no longer operational, so I cannot go and check.

THE COURT: So you didn't look into that information at all when you were investigating this matter, correct?

THE WITNESS: It would be a crime for me to visit the Playpen site, Your Honor, when it was up and running.

THE COURT: Excuse me. You can help me a lot -- if you answer questions, you can answer "yes" or "no" and make any explanation you desire. Otherwise, I may have trouble understanding your answers.

Now, let's go back over that. Let's go back. You say you don't know what the FBI knew when it was administering the site. Is that correct?

THE WITNESS: That is correct, sir.

THE COURT: So -- okay. Go ahead.

MR. GRINDROD: Thank you, Your Honor.

BY MR. GRINDROD:

Q. So this NIT, as the government has stated -- one of the -- is it your understanding that one of the reasons the government ran the NIT was to find out geographically where the user's computer was located?

THE COURT: He hasn't testified to that yet, and so be careful about leading the witness. I will allow it, because we pretty well know that he's been informed of a great many things, but don't lead witnesses, okay?

But that question I'm going to allow. I'm just warning you, don't do it again.

MR. GRINDROD: I'm warned. Thank you, Your Honor.

THE WITNESS: So the Tor software that everyone was using to access the Playpen site, that protects -- more than anything else, that is designed to protect the IP address of each person visiting the site.

THE COURT: So you're familiar with that software.

THE WITNESS: I'm familiar with Tor, yes, sir.

THE COURT: I understand you're familiar with Tor. Are you familiar with the software that Tor employs?

THE WITNESS: Yes, Your Honor, I'm familiar with the Tor browser, which is the software I think that we're discussing.

THE COURT: So you've looked at that software before.

THE WITNESS: I've used that software. The tool was created by the government ten years ago, and it's --

THE COURT: It's created by the Navy. Were you a part of that creation?

THE WITNESS: No, sir. It was created with by the U.S. Naval Research Lab originally and then was subsequently spun out into a nonprofit, but I've never been a developer of Tor or employed by the Tor organization.

But some of the developers taught classes at my Ph.D. university, and I know some of the developers who work on it.

THE COURT: My curiosity abounds. And what were their names?

THE WITNESS: Sorry. What was the question, sir?

THE COURT: You said you knew the developers because they taught you at the university. What were their names?

THE WITNESS: So Paul Siverson, who is employed by the U.S. Naval Research Lab still to this day, he was a visiting professor for a semester at my university.

THE COURT: And so he taught you a course?

THE WITNESS: Yeah, I think he gave one guest lecture in --

THE COURT: One lecture?

THE WITNESS: One lecture.

BY MR. GRINDROD:

Q. Dr. Soghoian, let me ask you about the government's -- so, again, going back to my original question, before the government deployed the NIT did the government have any understanding of where geographically an activating computer was located?

A. It would have been extremely difficult, if not impossible, because the Tor browser and the Tor network software are designed, first and foremost, to shield that information from everyone who might wish to discover it.

Q. And was --

THE COURT: Doesn't the person who is trying to get the information have to give the computer that it sends to information where to send the material?

THE WITNESS: So that's why Tor is such an interesting tool. When you use Tor to browse the Internet -- let's say you're visiting CNN, you look for an article on the CNN Web site. CNN doesn't actually know where they're sending it, so the data gets bounced around through a bunch of servers, and so no one --

THE COURT: How do they get the information, then?

THE WITNESS: If you --

THE COURT: It's not being sent back.

THE WITNESS: Instead of the data being sent directly from CNN to your personal computer, it gets sent through a couple intermediaries along the way, and they --

THE COURT: I know about coming to the Playpen. Now something leaves the Playpen, I assume.

THE WITNESS: Just as the connection from the user to the Web site goes through the intermediaries, the responses go back through the same intermediaries. And the intermediaries are servers run by volunteers around the world.

BY MR. GRINDROD:

Q. So before the NIT is deployed does the government have any idea where in the world the activating computer is located?

A. No.

Q. Okay. So I want you to imagine for me, then, a warrant that authorized the government to deploy this NIT but only against computers that were located in the Eastern District of Virginia. From a technological perspective, how would that warrant be executed?

A. There would be no way to limit the execution of a NIT to only computers located in the Eastern District of Virginia, because until the government hacks into the computers of the targets they won't know where they are -- I'm sorry. The government will not know where the defendants' computers are.

Q. Understood. I want to shift gears now for a moment and talk to you about some issues related to the pending motion to compel.

So at various points in the briefing the parties have referred to the NIT as having different components. Are you familiar with that terminology?

A. Yes, sir.

Q. Okay. In Mr. Eure's case, at least, the government has produced the two components of that, right?

A. Yes, the --

Q. Can you tell us what components?

A. I've reviewed and analyzed the NIT --

THE COURT: First tell us what two components they are, then you tell us what you analyzed.

THE WITNESS: Yes, Your Honor.

The two components are the NIT, the network investigative technique, and what's known as a PCAP, P-C-A-P, file. This is what the government, I believe, has referred to as a two-way network recording.

BY MR. GRINDROD:

Q. And two other components that exist but have not been produced, is one of those the exploit?

MS. YUSI: Your Honor, I object.

THE COURT: You know, I asked you not to lead the witness.

MR. GRINDROD: I'll rephrase, Your Honor.

THE COURT: I'm not going to do it anymore.

MR. GRINDROD: I'll rephrase, Your Honor.

THE COURT: Next time you'll know what happens, but don't do it again. And I asked you not to do it the last time.

MR. GRINDROD: I understand, Your Honor.

THE COURT: And I don't expect you to do those things if I tell you don't do it, okay?

He's perfectly capable of discussing it. He's been testifying. He's a volunteer. I'm not worried about him not knowing what's going on, but I am worried about leading the witness.

MR. GRINDROD: I understand, Your Honor.

BY MR. GRINDROD:

Q. You mentioned two parts of the four components. Can you tell us what the other two are?

A. The other significant components that are missing that I haven't reviewed and that haven't been disclosed are the exploit and the code that generates the unique serial numbers for the individual NIT deliveries.

Q. Okay. I want to talk about --

THE COURT: Slow down. One is called the exploit.

THE WITNESS: An exploit, yes, sir.

THE COURT: What is the other one?

THE WITNESS: The second one is a special code that would have run on the government's server that generated unique serial numbers each time the NIT was deployed.

BY MR. GRINDROD:

Q. I want to have you just --

THE COURT: And that is not the exploit?

THE WITNESS: No, sir. And if you would like, I can go through each component and say what they do.

THE COURT: I'm just trying to make sure where I'm going, because you're going to be discussing these terms. I want to be able to understand them.

Okay. Go ahead.

BY MR. GRINDROD:

Q. I do want to go through each of these components with you just to get an understanding of what they are, and then we'll talk later about why they may be important for various --

THE COURT: How much time do you expect for this witness?

MR. GRINDROD: It's going slower than I expected, Your Honor, but another half hour, at most.

THE COURT: All right. You have another half hour, period.

MR. GRINDROD: Thank you, Your Honor.

THE COURT: Because, otherwise, we won't get finished today.

MR. GRINDROD: I understand, Your Honor.

BY MR. GRINDROD:

Q. You mentioned the NIT computer code. Can you tell us what that is, briefly?

A. Yes. The NIT code has two pieces of functionality. The first is that it collects specific information from the computers on which it runs. That might be the serial number of the Wi-Fi card, information about the operating system that's running on the computer.

Once it has compiled that information, the second piece takes over, and that transmits that collected information back to an FBI-controlled server.

Q. The PCAP data, can you tell us what that is?

A. The PCAP data is a recording created at a government facility that purports to show what the government received from the individual NIT users.

Q. The exploit, what is that?

A. As I said before, the Web browser that people are using, that is designed to visit Web pages, and the Tor browser is a special Web browser that is designed to be more secure than the average Web browser.

The piece of information that it is designed to protect, first and foremost, over everything else, is the IP address of the user. The Tor browser is designed so that if a Web site asks, "What is your IP address?" it will say, "No," and it is designed to resist any creative attempts to try and learn the user's IP address.

For the NIT to be able to successfully run on the computer of the targets, the first thing the government needs to be able to do is to somehow bypass these strong security features built into the Tor browser. And, so, if you think of the Tor browser as a house guarded by trained guard dogs, the exploit is a piece of meat that's been laced with sleeping pills so the guard dogs fall asleep and let the government go inside the house. So the exploit is the code that bypasses or circumvents the security settings and protections in the Tor browser.

Q. And then the final piece is the unique ID generator --

THE COURT: The exploit is the thing that tells them what computer is coming in on that particular information?

THE WITNESS: No, Your Honor, the NIT is the code that identifies the computer and sends that information back to the FBI server.

The exploit is the code that disables the security protections of the Tor browser so that the NIT can then be installed and execute.

BY MR. GRINDROD:

Q. So if the question is what let you in --

THE COURT: Hold on a minute.

BY MR. GRINDROD:

Q. What's the -- what let you in or what allowed the government --

THE COURT: Stop a minute so I'll understand where we're going.

First you find the name of the computer; that is, the individual computer?

THE WITNESS: No, Your Honor. That's actually one of the later stages.

The first thing the government has to do is get the defendants' computers into a state where they will allow the NIT to run. Normally, the Tor browser software will refuse to run something like the NIT, because first and foremost it's designed to protect that information from outside parties who might wish to learn it.

So the exploit has to disable the built-in security features that are contained within the Tor browser, and it does that through the use of what is called a security vulnerability; that is, a design mistake in the software, in the Tor browser software.

The Tor browser, like all pieces of software, is made by humans --

THE COURT: So the exploit just destroys, in essence, any security; that's it.

THE WITNESS: That's a good way of thinking of it, sir, yes, sir.

THE COURT: All right.

BY MR. GRINDROD:

Q. Okay. And then the last component of the four is the unique ID generator. Can you tell us briefly what that is?

A. Yes. The purpose of the ID generator -- when the defendants or the targets visit the Playpen site and receive the NIT and the exploit, they are given a unique number like a serial number.

When the computers that are running the NIT call home, in addition to transmitting back their serial numbers and other information, they transmit back that number that the government has given them. In essence, it allows the government to associate a particular user on the Playpen site with a particular successful operation of the NIT and, as a result, the IP address that the government learns through the NIT operation.

Q. Okay.

A. And it's through the unique numbers that they're able to say, defendant X was this user name on this Web site, and they were logged in for this many days, and they viewed these posts. That gives them the ability to identify individual users and their history on the sites.

Q. Understood. So let's focus first on the exploit.

Can you tell the Court why it's important from a technological perspective to review the exploit? What would that tell you?

A. The exploit is important for a few reasons. The NIT collected a bunch of information from the computer, and without knowing -- without experts being able to look at the exploit, it's not possible to say which condition or state the computer was in before it collected the NIT.

Let me use an analogy. If the government is analyzing DNA in a lab, you want to know that the petri dishes that they were using, the equipment in the lab, is clean. You want to know that it's sterile before they test a particular defendant's genetic sample.

If we cannot see the exploit, we do not know the state in which the computer was in before it ran the NIT, which calls into question the reliability, the forensic reliability, of the evidence that the NIT then collected. So that's the first reason.

THE COURT: So looking at any computer, you have to know what it was before anything was done to the computer. Is that correct?

THE WITNESS: It would certainly be helpful. If you want --

THE COURT: I didn't ask you about "helpful." Everything is helpful.

The question in my mind is if I were looking at a computer, any computer -- let's forget this case. We're talking about your expertise. If I were looking at a computer and wanting to know what it's putting out, I'd have to know in advance what it had on it before?

THE WITNESS: That is true. You would want to know --

THE COURT: So nobody should ever be able to testify what was on a computer, correct?

THE WITNESS: The --

THE COURT: They can't testify because they couldn't possibly have known what was on it before, even if they looked at the computer, correct?

THE WITNESS: There are many things that a computer can do, but the --

THE COURT: I understand there are many things a computer can do, and I can walk and run and talk and count to ten, but that doesn't mean that I can't ask questions concerning what's happening.

What I'm trying to find out is -- the statement you're making is that unless I know what was there before I cannot tell you what's there after.

THE WITNESS: If I could try and explain --

THE COURT: So anything I see is not real, because it could have been different.

THE WITNESS: The --

THE COURT: I couldn't say that Mr. Grindrod is there unless I knew he wasn't there yesterday, correct?

THE WITNESS: The exploit forces the computer to do things that it would never normally do, and it puts -- it stresses the computer or the software running on the computer --

THE COURT: I know what the exploit does. This is not the first case, by the way, and we've heard these terms consistently.

And what I want to do is to make sure I understand what you're saying in relation to the determination of how the FBI learned of whose computer was calling their Playpen site. And you're saying that the first way they learned is by having the NIT, having exploit, that would allow them to find the name of the individual calling, correct?

THE WITNESS: It's not the name of the individual --

THE COURT: Well, the name of the computer.

THE WITNESS: The name of the person logged in to the computer, the unique serial number associated with their Wi-Fi card, and some other information from the computer.

THE COURT: So all of this is generated towards finding out that particular computer, correct?

THE WITNESS: You're asking me if that's why the information is collected by the NIT?

THE COURT: Yes.

THE WITNESS: I believe that is why the FBI collects information from those computers, yes, Your Honor.

THE COURT: All right.

BY MR. GRINDROD:

Q. So I think you mentioned --

THE COURT: I'll give you five minutes more by virtue of the fact that I've interrupted you.

MR. GRINDROD: Thank you, Your Honor.

BY MR. GRINDROD:

Q. So you mentioned one of the reasons why it's important to view the exploit, but I think you said there were other reasons.

A. There's another significant reason that you would want it. If you think of the computer as a house, you have a front door, you have a lock on the door. As I said, the exploit takes advantage of a security flaw in the software that was there that most people may not have known about ahead of time. So think of it as a design flaw in the lock on your front door. So the government knows that there's a flaw in your lock so they send a Special Agent who is skilled in the art to stand there and pick the lock, and that gains them access to your house, and then they can execute the search inside the house.

Now, you could pick the lock, if you're skilled at lock-picking, and leave no trace, and when you close the door and you're done with the search the lock is in perfect working order. But it's possible if you make a mistake you could still gain access to the house, but you could break the lock in the process, and then the lock may not work in the future and other people could go inside that house after.

One of the reasons why it would be a really good idea for the defense to be able to look at the exploit is to see if the exploit leaves the computer in as secure a state as the government found it or if it leaves the computer in a more vulnerable state, where other parties might be able to log in to the computer, download their own software to the computer, download other content or contraband to that computer.

And this is not a hypothetical concern. Tools similar to NITs used by other governments have been analyzed by experts, and --

THE COURT: Stop telling me unless you give me -- you know, the world is full of explanations, so we've got to deal with specifics. Who did what to whom at what time?

THE WITNESS: Okay. So a specific example:

A tool like the NIT, used by the German police, was analyzed a couple years ago by German security experts and discovered to have security flaws in it that left the targets of the authorized law enforcement investigations -- left those computers vulnerable to compromise and search by unauthorized third parties.

It is very difficult to design secure software, and it's quite possible that the exploit may have flaws in it that we don't know about, but if it left the computer in a less secure state it's possible that other parties might have been able to gain access to that computer at a later date.

THE COURT: So why would another party want to gain access?

THE WITNESS: Your Honor, there are --

THE COURT: I didn't ask -- is there any evidence that some other party tried to gain access? Did you hear of any?

THE WITNESS: So criminals break into computers every day.

THE COURT: I know that, but they generally break into computers because they want to find out something, correct?

THE WITNESS: No. There are many reasons why criminals do it.

One frequent reason is not to steal information from a computer but to use that computer as a staging point to download and distribute other stolen information.

THE COURT: To break into that, wouldn't they have to be able to know what it is they're breaking into?

THE WITNESS: No, Your Honor, there are tools that one can use to scan the Internet for vulnerable computers, so --

THE COURT: If you scan the Internet, how many millions of computers are there?

THE WITNESS: There are a large number of computers in the world, but there are tools that can scan the entire Internet in less than an hour.

THE COURT: In less than an hour?

THE WITNESS: Yes, sir.

THE COURT: So what do you scan the Internet, and what does it give you?

THE WITNESS: So there's a tool that was made by the University of Michigan called ZMAP, Z-M-A-P, that can visit and interact with every single computer on the Internet in less than an hour. And think of it as knocking on the front door of every house on the street.

THE COURT: What does it do?

THE WITNESS: It makes a connection to a computer, and a follow-up activity would be looking for known flaws, looking for likely methods of entry. So, you know, a criminal might try and open the window on every front door -- or the front window of every house on the street.

THE COURT: So what you're saying is if they had unlocked the computer, if they unlocked the door to this house, a person could scan it, every computer in the world, in one hour. And then what would that do?

THE WITNESS: They could gain access and do --

THE COURT: And do what?

THE WITNESS: Sorry?

THE COURT: How does it change what already has occurred?

THE WITNESS: It's not that it changed what has already occurred, it's that they could -- the information that is on the computer could then be changed by subsequent people entering the house.

THE COURT: The information on the computer. So the information concerning the address would be changed?

THE WITNESS: Not the --

THE COURT: Right now we're talking about getting the address or the computer of the individual concerned.

THE WITNESS: It's not --

THE COURT: It wouldn't change that, because the FBI already has it, don't they?

THE WITNESS: The user name on the computer, the identifiers, those wouldn't change, but any contraband the government later discovered in an in-person search --

THE COURT: Well, first we're dealing with the question of finding out whose computer it is that's communicating with Playpen. They find that. Then you're saying, well, they need to know the exploit, because it could tell us what happened subsequent to that, correct?

THE WITNESS: Yes, Your Honor.

THE COURT: Couldn't tell us what happened before that.

THE WITNESS: The -- so, as I said, there were two main reasons for the defense to look at the exploit --

THE COURT: I understand that. They could put something in there and put it into Tor -- into Playpen.

THE WITNESS: No. So the latter reason is the reason -- as I just discussed, would go to what may have been found on the computer weeks or months later.

The former reason, you know, knowing the state that the computer is in, that goes to the validity of the information that the NIT collects.

THE COURT: So what you're saying is that they couldn't -- there's no way to rely on a name that they obtain, and that would be wrong. Is that correct?

THE WITNESS: So there is a unique identifier on the computer called a MAC address, and that was one of the things collected by the NIT. It's a serial number for your Wi-Fi card burned in at the factory. That can be changed by software running on your computer, and so --

THE COURT: It can't be changed until you get to the computer.

THE WITNESS: That is correct.

What I'm saying is if the exploit somehow malfunctioned it's possible that that serial number might have changed in such a way that it would be, you know, forensically unreliable.

THE COURT: All right. Go ahead.

BY MR. GRINDROD:

Q. Let me ask you about the second reason you stated, which was the one that had to do with changes to the computer potentially after the NIT was deployed.

Does the time gap between when the NIT was deployed and when the computer was physically seized in a traditional search, does that affect anything as far as, you know, the mistakes of that second reason?

A. There are a lot of criminals out there on the Internet who try and break into computers, and the longer that a computer is left vulnerable to cyber attackers the greater opportunity those cyber attackers will have to compromise the computer and use it for whatever purpose they have.

If someone -- you know, if the FBI were to show up the day after the NIT operation, that would be a relatively short window. If they waited a year or 11 months to conduct the search, that would be a lot of time for a vulnerable computer to be compromised by other third parties.

Q. Have you reviewed Agent Alfin's declaration in this case that was also filed in the Matish case?

A. I have.

Q. So in paragraph 9 of that declaration Agent Alfin essentially states that he executed the exploit and observed that it didn't make any changes to the computer.

Do you have any views on that statement?

A. I do. I --

THE COURT: I -- well, go ahead. No objection?

MS. YUSI: (Shakes head.)

THE WITNESS: So Special Agent Alfin testified saying, essentially, that the exploit worked just fine; that he ran it on his computer a few times, it worked okay in the lab, and there's no reason to believe that the exploit malfunctioned and, as a result, there's no need for the defense to be able to look at the exploit.

It's really hard to write reliable, secure software. Large companies like Microsoft and Apple and Boeing, spend a huge amount of money on software quality assurance, trying to write code that does what they think it's supposed to do. They also employ teams of people who do nothing but test the software to look for flaws. And they don't just run it once or twice, they run it thousands or millions of times, looking for that one-in-a-million case where it misfires or does something unpredictable.

It is frequently the case that software can have subtle flaws that don't show up under a modest amount of testing, and, you know, with respect to Special Agent Alfin's declaration or testimony, running an exploit a couple times is not enough to say conclusively that it works and that it didn't have any bugs, particularly if he hasn't even looked at the exploit, which is my understanding from that testimony. You know, even when experts can look at codes, sometimes they don't notice flaws. This is why we have, you know --

THE COURT: So experts can differ.

THE WITNESS: Experts who have access to the same information can differ, but in this case only one side has access to the information, and we have to take their word for what the code does.

BY MR. GRINDROD:

Q. So, Dr. Soghoian, let me direct your attention to another component, which we talked about earlier, called the PCAP data.

Now, in this same declaration that we were just talking about, Agent Alfin's declaration, he, in paragraph 16, said that the data stream reflecting the information transmitted to the FBI from the defendant's computer --

MS. YUSI: We object, Your Honor; leading.

THE COURT: Objection sustained. You may recite exactly what he said.

MR. GRINDROD: Okay. Thank you, Your Honor.

THE COURT: Don't start summarizing --

MR. GRINDROD: I'm sorry. I was trying to --

THE COURT: -- because then you are changing, in some ways, it. Let him understand what it is. You can say, "He says as follows," and I'll allow you to do that, but don't --

MR. GRINDROD: Thank you, Your Honor.

THE COURT: "In essence, he says this."

MR. GRINDROD: Thank you, Your Honor.

THE COURT: In essence, I might say one thing, but the question is what it is that's exactly said.

BY MR. GRINDROD:

Q. So paragraph 16 of Special Agent Alfin's declaration reads as follows:

"Review of this data stream reflecting the information transmitted to the FBI from Matish's computer as a result of the deployment of the NIT confirms that the data sent from Matish's computer is identical to the data the government provided as part of discovery."

Have you reviewed the PCAP data in Mr. Eure's case and other Playpen cases?

A. I have. I've reviewed the PCAP in this case and one previous case.

Q. In your view, is Special Agent Alfin's statement in paragraph 16 that I just read to you -- is that statement correct?

A. No, in my view it is not. The PCAP -- the recording of the data that the government received only shows what the government received, it does not show what the NIT sent.

So think of it this way: You have someone putting a letter in the mail, it goes through the U.S. Mail system, and the government has a video camera pointing at the FBI's office showing the letter being delivered. Their recording doesn't show what happened along the way as the letter was making its way from point A to point B, it doesn't show who may have opened the letter, it just shows what happens once the government has received --

THE COURT: So if you received any e-mails from anyone it would have the same problem. It could be different -- if you received it, it could be different from what was sent, correct?

THE WITNESS: And, for that reason, there is technology that you can use to protect against that.

THE COURT: I understand that, but I look at e-mails all the time; I assume that they're what somebody sent. And you're saying you shouldn't assume what somebody sent because it could be changed along the way.

MR. GRINDROD: Can I follow up on that, Your Honor?

THE COURT: Certainly.

BY MR. GRINDROD:

Q. So clarify for me. Is this a theoretical possibility that this information was changed, or can you testify that, in fact, information in the PCAP data stream was changed?

A. Looking at the PCAP data stream, there are indicators in there showing that at least some of the information was changed as it was transmitted from A to B.

THE COURT: What was changed?

THE WITNESS: The IP address of the government server that is in the PCAP recording is definitely not the IP address that was -- that the NIT addressed the information to when it left the defendants' computer.

THE COURT: Excuse me. The NIT addressed the information to a different computer than that which was sent back to them?

THE WITNESS: Your Honor, I'll try and explain it in English to you, in plain English.

If I call your chambers --

THE COURT: Yes.

THE WITNESS: Let's say I have a telephone number. I call your chambers, and I ask to speak to you.

THE COURT: Yes.

THE WITNESS: I'll speak to one of your colleagues, and then they will transfer me on an extension to your chambers.

THE COURT: Correct.

THE WITNESS: I may not know your direct line. In the same way, the PCAP file does not have the extension of the server that actually received the data -- sorry.

The PCAP file contains the extension number, it doesn't contain the number of the main switchboard, and only the main switchboard number was reachable from the outside world.

THE COURT: So the government server that got the IP or the exploit was not the government server that sent back the information.

THE WITNESS: That's also true. There was a server that the government maintained that delivered the exploit, and then there was a different server that received the information back from the NIT, but then there's also a third government server --

THE COURT: Stop a minute.

First we have Playpen, okay?

THE WITNESS: That's a government server, yes, sir.

THE COURT: That's a government server. I thought the exploit got you into the Playpen.

THE WITNESS: The exploit was delivered when someone visited Playpen and caused the NIT to operate, which calls home to a second government server.

THE COURT: Okay.

THE WITNESS: Then that second government server passes the information to a third government server, and that third government server's address is in the PCAP recording.

THE COURT: So, similarly, there are several computers involved, is what you're saying.

THE WITNESS: The second IP -- the second server's address, which is the one that the NIT would have called home to, that never appears in the recording. So that IP address was changed. As the information was being passed from server number two to server number three the IP address was changed, and the recording that we've been given only lists server number three.

THE COURT: Okay. So the information being transmitted back from the Playpen to the ultimate user of the information -- that is, the person desiring the particular documents or pictures that Playpen has -- it goes through several different computers constantly in order to hide where it came from or where it was going.

THE WITNESS: That is correct, Your Honor.

THE COURT: So this is not unusual, then, for information to go from one computer to another.

THE WITNESS: If I might expand on what you're asking, the ---

THE COURT: I'm merely asking how does the person know that what they got is what was sent?

THE WITNESS: I have a good answer for that.

THE COURT: Oh.

THE WITNESS: So there's a technology called "encryption." If you've ever visited your bank's Web site, you'll see a lock icon, and that's designed to do two things. It protects the confidentiality of information so that no one can see your account number, but it also stops anyone from tinkering with the information as it's sent from A to B. The connection from Playpen to the visitors to the site was encrypted, and so nothing could be tinkered with as it was going from A to B.

The connection from the NIT users back to the FBI was not encrypted, and so when the NIT called home the government did not have a chain of custody of the data that the NIT sent, and it could have been tampered with along the way. Now, they knew how to maintain the chain of custody because they used it for the outgoing data from the Playpen site to the user, but they didn't use it on the way back.

And in your question about e-mails, it used to be a big problem on the Internet that people would receive e-mails that purported to be from other organizations. You could get someone trying to steal your banking credentials by pretending to be Bank of America or Chase. And now all of the big Internet companies actually employ some encryption technology that signs e-mails so that only Bank of America can send e-mails that look like they come from Bank of America, and if someone tries to fake it they go straight in the trash can.

BY MR. GRINDROD:

Q. So I want you to imagine for me now that you were at trial in this case and either Special Agent Alfin or some other government expert testified, in sum and substance, to what is in paragraph 16.

Would you testify to something inconsistent with that?

MS. YUSI: Objection, Your Honor. This calls for speculation as to --

THE COURT: I'm going to allow him to testify what's wrong with it.

THE WITNESS: I disagree with Special Agent Alfin's assessment of what the PCAP file -- what the recording shows. I believe it does not show what the NIT sent, I believe it only shows what the government received.

And, moreover, Special Agent Alfin --

THE COURT: So you can't tell what was sent because -- you're saying the possibility that there was some invasion or hacker that came in -- they could change whatever was sent so that the identification of the computer of the defendant was not the defendant's computer.

THE WITNESS: That possibility is there, and --

THE COURT: Except if they went to the defendant's computer and saw it then it wouldn't make any difference to you at all?

THE WITNESS: That's a legal question, Your Honor.

THE COURT: Oh, it's a legal -- what's legal about it?

THE WITNESS: You're not asking me --

THE COURT: I'm asking you. You're the expert testifying here, and I'm saying, as an expert, if the information you received is what you saw, then you still feel that a hacker changed it?

THE WITNESS: I'm not saying that a hacker has changed this stuff, Your Honor, I'm saying that the government had the means to maintain a chain of custody, and they didn't use it.

THE COURT: Oh, unquestionably. I have the means to maintain a lot of things that I don't maintain, and what you're saying is in this case they didn't utilize encryption in transmitting information. Is that correct?

THE WITNESS: That is true.

THE COURT: Okay. But that's not to say that the information transmitted was incorrect, that's to say there's a possibility that it could be incorrect if a hacker invaded it and what they saw when they got there was different from that which was transmitted.

But if it wasn't different...

THE WITNESS: So, separately, Special Agent Alfin testified that the data that left the client is exactly the data that was received by the government, and, as I just testified before, the IP address information did change along the way.

THE COURT: Okay. Go ahead.

BY MR. GRINDROD:

Q. So would you be able to have reached that conclusion had you not analyzed the PCAP data?

A. No. Within five minutes of looking at the PCAP data it was clear that there was something wrong, but without the PCAP data the only thing I would have had to go on was Special Agent Alfin's testimony saying that nothing changed.

Q. The question may come to someone's mind, why not conduct a forensic analysis of the defendant's computer. So does that move the ball forward one way or the other in answering these questions that you've raised about the exploit?

MS. YUSI: Your Honor, I'm going to object. He's not a forensic expert. He's talking about a NIT, and that's his specialty.

THE COURT: He's a computer expert. I understand that.

MS. YUSI: I'm not sure --

THE COURT: I'll allow him to testify as a computer expert, not as a forensic expert.

BY MR. GRINDROD:

Q. Do you remember the question?

A. No. Can you say it again?

Q. Sure. So the question may come to mind, why not look at our clients' computers.

THE COURT: Not "why not." Ask him a question.

MR. GRINDROD: Okay. So --

THE COURT: Don't ask him why not.

MR. GRINDROD: Okay.

THE COURT: Please, don't.

BY MR. GRINDROD:

Q. Would a forensic analysis of the hard drives of the computers in this case --

THE COURT: Stop. He just said no forensic testimony, and I agreed. He's not claiming to be a forensic expert, he's claiming to be a computer expert, and you just -- what a forensic -- do you see what I'm trying to tell you? Let's don't get into that.

BY MR. GRINDROD:

Q. So you've addressed certain questions that -- and talked about how the exploit may shed light on certain answers. Is there anything about looking at the computers themselves in this case that would answer those same questions?

A. It would be very difficult. The longer the time period between when the NIT and the exploit executed and when the computer was searched and ultimately a forensically sound copy of the computer was made -- the longer that period is, the more time there is for information on that computer to deteriorate.

If the government had conducted the search of the defendant's house an hour after the NIT operated and the computer hadn't been turned off, you know, you'd probably have a pretty good idea of what happened. But if it's been months and the computer has been turned off frequently, a lot of information would have been lost, particularly if much of what the NIT and the exploit did only tampered with the software that was running on the computer and not the software that was installed permanently on the computer.

And, so, it would be really hard to reconstruct what happened a year before just by looking at the physical computer, without being able to look at the individual components of the government's software that ran on the computer.

Q. Let's talk quickly about the last component that has not been produced, the unique ID generator.

You told us what that is, but can you tell us why that's important, from your technological perspective?

A. Sure. As I said before, the purpose of the ID generator is to allow the government to associate a known user on the Web site, someone with user name Jack, with a particular IP address that is revealed through the NIT.

For that to be -- for the ID generator to be helpful, it must generate a unique ID only once. If it malfunctions for some reason and generates the same ID over and over again, you could incorrectly associate one user's activity on the site with a different person's IP address.

Q. Other than looking --

THE COURT: Well, was there any evidence that there was multiple deliverance of the same site?

THE WITNESS: Well, there's certainly hundreds --

THE COURT: I didn't ask you that. Was there any evidence in this case? I don't remember any declaration saying that. Where do we get this? Is there any evidence of this?

MR. GRINDROD: I'm sorry. Any evidence of what, Your Honor?

THE COURT: Just what he testified to.

MR. GRINDROD: Well, Your Honor, we haven't been provided with the evidence. We haven't been provided with a unique identifier, so we don't --

THE COURT: Well, how is he testifying as an expert on that which he doesn't know any evidence of?

MR. GRINDROD: He knows what --

THE COURT: It makes suppositions, but I don't want to start talking about evidentiary matters. When we start dealing in that we're dealing in a different scope. He's an expert. Not a forensic expert, but a computer expert. And I am assuming that he is a computer expert.

MR. GRINDROD: Well, this --

THE COURT: The question in my mind is -- the only question I'm trying to find out is where we're going.

MR. GRINDROD: I --

THE COURT: The question really before us is did the government violate Mr. Eure's constitutional rights.

MR. GRINDROD: Well, Your Honor, we're --

THE COURT: That's one question we're dealing with, and so far I've heard very little about that. I've heard a lot about the computer. So eventually we're going to start talking about something that's evidentiary in this case.

We allowed an expert to testify, and I did it out of order, without any evidence at all other than the evidence in the declarations. And we can do that because this is not a trial of any sense but a question of the appropriateness of various search warrants.

MR. GRINDROD: Well, Your Honor, we're also --

THE COURT: And I assume we are dealing first with Mr. Eure's warrant that you're trying to suppress the evidence. Now, what evidence are you trying to suppress?

MR. GRINDROD: None with this, Your Honor. I'm sorry. As I tried to flag for the Court, I had moved on to the motion to compel. These are trial --

THE COURT: Oh, you're not -- the only thing in the motion to suppress, then, was what was on his computer?

MR. GRINDROD: Was the -- well, Your Honor, to the extent -- Your Honor, basically, the testimony that I offered with respect to where the NIT was installed, the geographic location, and also as to how the NIT would have worked had the warrant only authorized it being deployed on computers that were located in the Eastern District of Virginia. Those were the topics that were specifically directed to the suppression.

THE COURT: So all of this testimony that he has, other than that very short testimony, deals with the motion to compel.

MR. GRINDROD: That's correct, Your Honor.

THE COURT: I got lost on the motion to suppress. And so all of this deals with the motion to compel them to produce what?

MR. GRINDROD: To produce the exploit and the unique ID generator.

THE COURT: The code is what you want, correct, the code that allows them to get into Tor?

MR. GRINDROD: The code that allowed them to get into our client's computer. They were operating the Playpen server on Tor, but --

THE COURT: So what you're seeking to suppress is exactly what? So tell me.

MR. GRINDROD: Well, with respect to suppression, it's everything that was a fruit of the NIT.

THE COURT: Everything is nothing, so tell me what it is you're seeking to suppress.

MR. GRINDROD: Your Honor, we're seeking to suppress all fruits of the NIT search. And that's how they identified our clients in these cases, so it's everything. I mean, I don't mean to be cavalier --

THE COURT: Well, normally if we have a weapon we want to suppress the utilization of the evidence.

MR. GRINDROD: Correct.

THE COURT: If it's the subject of a seizure, that was the subject of an illegal search and seizure. Evidently, they seized or obtained evidence by a search.

MR. GRINDROD: That's correct.

THE COURT: And you're seeking to suppress what? That's all I'm asking.

MR. GRINDROD: To suppress the evidence of the -- obtained by -- I'm sorry, Your Honor.

THE COURT: What evidence? What gun, weapon, anything else? Tell me what it is you're seeking to suppress.

MR. GRINDROD: We're seeking to suppress the hard drives, the -- we're seeking to suppress the information --

THE COURT: The hard drive is not in evidence. It's not -- what difference does that make? It's what information was taken from the hard drive.

MR. GRINDROD: Any and all evidence from it, Your Honor.

THE COURT: What information are you seeking to suppress, is what I'm trying to get at.

MR. GRINDROD: If I could --

THE COURT: When we suppress something we have an object to suppress; a PIN, the wording of such-and-such and so-and-so, this particular evidence.

All I'm asking is what evidence are you seeking to suppress?

MR. GRINDROD: We're seeking to --

THE COURT: When you say, we're seeking to suppress all evidence of his guilt, that's wonderful, but it doesn't help me a bit. It doesn't help anyone.

So what are we seeking to suppress?

MR. GRINDROD: Testimony about our client's alleged activity on the Playpen Web site, testimony regarding -- Your Honor --

THE COURT: That's not a motion to suppress. You've got to suppress some evidence. What evidence are you seeking to suppress?

MR. GRINDROD: The IP address mainly, Your Honor.

THE COURT: I understand you're seeking to suppress anything that might lead to your client being guilty, and I understand that, but that is not a motion to suppress. You've got to suppress something.

MR. GRINDROD: We're seeking to suppress the IP address, the MAC address --

THE COURT: Wait a minute. You're seeking to suppress the IP address of the defendant, correct?

MR. GRINDROD: Correct.

THE COURT: What else?

MR. GRINDROD: The MAC address.

THE COURT: The MAC -- what's the MAC address?

MR. GRINDROD: It's the unique code that appears on any wireless card, so it would have been the code associate with the device our client used to access the Internet. It was obtained through the use of the NIT.

THE COURT: You're trying to suppress what your client's code was?

MR. GRINDROD: Yes, Your Honor.

THE COURT: Client's code.

MR. GRINDROD: The host name, Your Honor, the operating system.

THE COURT: You can't suppress a system. You can suppress something.

MR. GRINDROD: Suppress any testimony regarding what operating system was running on any computer associated with --

THE COURT: You want to suppress any evidence of any operating systems on any computer or a particular computer?

MR. GRINDROD: On the computers mentioned in the forfeiture allegations in this case.

If I may, Your Honor, I don't mean to make an end run at all around the Court's desire to get specific about this, but if I could just very briefly explain why I think it is -- why the --

THE COURT: No, don't explain anything. The witness is on the stand. Let's keep going.

MR. GRINDROD: Understood, Your Honor.

THE COURT: You've got five minutes, and that's it.

MR. GRINDROD: Understood, Your Honor.

THE COURT: The ball game's over.

BY MR. GRINDROD:

Q. We were talking about the unique ID generator. Is there any other means of determining whether multiple IDs were created that matched, other than having the generator itself?

A. The government's server would know which IDs were sent back, so the government has in their possession a list of NIT clients that called home and what their unique IDs were. But some of the NIT clients would never execute properly, so there would be failures. And so there's no way of knowing, without looking at the generator, if the generator would have executed successfully, if it did what it was supposed to do and gave unique codes to everyone.

THE COURT: What is the ID generator?

THE WITNESS: So this is the code that creates serial numbers for each operation of the NIT.

THE COURT: "This is the code." The ID generator is the code?

THE WITNESS: Yes, Your Honor.

THE COURT: So without knowing the code you don't know what the government's position was.

THE WITNESS: Without knowing the code you don't know if the ID numbers were created properly. In a successful, good operation you would want one new code for each delivery of the NIT. If that code malfunctioned and gave two people the same ID, that would be a bad thing.

THE COURT: Except we have no evidence of any malfunction. That's a supposition you're making. If that occurred something would be different, correct?

THE WITNESS: That's why it's useful to have the code.

THE COURT: If it occurred, something would be different, correct?

THE WITNESS: Yes, Your Honor.

THE COURT: All right.

BY MR. GRINDROD:

Q. Let me jump back and talk to you briefly about the exploit one more time.

To your knowledge, has the FBI disclosed the exploit in this case to anyone?

A. Sure. When the operation took place the government would have provided the exploit to hundreds of thousands of people. When the operation took place the exploit was delivered to every person who the government delivered the NIT to.

Q. Was there any way for someone to capture the exploit or record it?

A. Sure. Just as the government can make a recording, a PCAP file, on their end and record the data that they receive, so, too, can individuals record a copy of all the data that they receive from the Web sites that they visit.

And in a previous NIT operation that the government did in 2013 a copy of the exploit that they used then was -- the exploit and the NIT were saved by experts who visited the Web site that was being used for the NIT delivery, and the government's exploit and NIT were analyzed by independent experts.

So the government has in the past, through unfortunate luck, had their NIT and their exploit analyzed by the open research community.

THE COURT: This particular NIT was -- this exploit was analyzed?

THE WITNESS: No, Your Honor, a different one that they used in --

THE COURT: A different exploit.

THE WITNESS: -- in 2013.

THE COURT: In 2013.

THE WITNESS: This operation took place in 2015, but two years before that the FBI seems to have made a mistake, and their NIT was delivered to people who were not themselves viewing contraband, and some of those individuals saved copies of the NIT and published it online.

MS. YUSI: Your Honor, I'm going to object to his speculation as to any mistake that was made.

THE COURT: I'm going to allow him to testify for what it's worth, ma'am, okay? Let's go.

MR. GRINDROD: I have no further questions at this time, Your Honor.

THE COURT: All right. You have 50 minutes for cross-examination. We're going to have to come back tomorrow morning, it looks like.

MS. YUSI: I'm sorry, Your Honor. You said we only have 15 more minutes?

THE COURT: 50 minutes.

MS. YUSI: Okay, Your Honor.

THE COURT: Wait a minute.

Mr. Cejas, in relation to your portion of this testimony, do you want to ask any more questions of this --

MR. CEJAS: No, sir.

THE COURT: All right. Anything that hasn't been asked. All right. Let's go.

MS. YUSI: Your Honor, I have an agent here. I have Special Agent Alfin here from D.C., so I'm hoping we can get him on briefly today.

THE COURT: Okay.

CROSS-EXAMINATION

BY MS. YUSI:

Q. Dr. Soghoian, you said you're pro bono here, but you're not here on behalf of the ACLU, correct?

A. That's correct.

Q. Do they support you being here?

A. What does that mean?

Q. I mean, did they approve? Did you ask to be here on their behalf?

A. Not on their behalf. I was told, in fact, that for the NIT work that I've been doing, the unpaid NIT work, that I should emphasize in each case that I'm doing this in my personal capacity and not on behalf of the ACLU.

Q. Okay. Your supervisors told you to not associate the ACLU with what you're here for today?

A. And when I speak on panels at conferences I'm also told to say that, just like government employees.

Q. All right. Now, you agree that the TOR project doesn't promise perfect security to its users, correct?

A. I believe there's a statement on the Tor Web site that acknowledges risks associated with the Tor software, yes, ma'am.

Q. And Tor is used by a lot of people, but it includes criminals who commit crimes, correct?

A. I believe that's true.

Q. Do you believe that, or do you know that to be true?

A. I don't know any criminals that have used Tor, but --

Q. But you've testified in a lot of criminal -- well, this particular --

A. This is my third case.

Q. Okay. But you're aware that Tor has been used by criminals, based on news reports and things like that.

A. Yes, ma'am.

Q. Okay.

THE COURT: You didn't know that child pornography was criminal?

THE WITNESS: I'm aware that child pornography is a crime, but I don't have firsthand knowledge -- I only have -- I've read the newspapers --

THE COURT: You don't have firsthand knowledge of any of this, sir, you only have knowledge that was based on what your investigation was. And your investigation did not reveal any criminal activity?

THE WITNESS: The --

THE COURT: You mean you didn't see anything about child pornography in this case?

THE WITNESS: Your Honor, I haven't looked at any child pornography in this case.

THE COURT: Nobody told you what this case was about?

THE WITNESS: I've certainly read the affidavits in this case, but I haven't looked at any of the child pornography, if that's what you're asking.

THE COURT: The affidavits mean nothing. That's the evidence in this case, correct?

THE WITNESS: The --

THE COURT: You didn't analyze anything from the affidavits. Even as a human being you didn't realize that this was all dealing with child pornography?

THE WITNESS: So my understanding -- so the three cases --

THE COURT: Your understanding is child pornography is not a crime?

THE WITNESS: Your Honor, the three --

THE COURT: You testified that this wasn't criminal activity.

THE WITNESS: The three cases in which I've testified, none of them have led to convictions yet, so I don't personally know --

THE COURT: So it's not a crime unless someone is convicted of it, correct?

THE WITNESS: I'm not a lawyer, Your Honor, but that's --

THE COURT: Just so I understand what you're saying -- you know, the problem is -- the only thing that's criminal is if there's a conviction? If somebody shoots another person and they don't convict them, it's not criminal, correct?

THE WITNESS: I don't know, Your Honor. I'm not an expert on that.

THE COURT: You don't have to be an expert to understand what murder is, do you?

THE WITNESS: (No answer.)

THE COURT: You know, I'm not trying to do anything except find out...

Go ahead. I'm sorry, Ms. Yusi.

BY MS. YUSI:

Q. You agree that law enforcement -- their job is to stop crime, correct?

A. That is one of their jobs, yes, ma'am.

Q. All right. And they have an obligation to stop crimes, including sexual exploitation of children on the Internet.

A. Yes, ma'am.

Q. And they need to stop and identify these criminals through legally available means, correct?

A. I'm sorry. Can you ask that question again?

Q. Do you agree that law enforcement should stop the exploitation of children on the Internet through legally available means? Do you agree with that?

A. Yes, if those means are lawful.

Q. Okay. But you also agree that your purpose is to also fight government surveillance, right?

A. Yes, ma'am -- well, I believe that my role is to help our democratic system keep surveillance under control.

Q. Okay. And to fight surveillance?

A. That is what I do through my actions as someone who helps the courts and legislative bodies adequately oversee surveillance tools that are frequently used in the shadows.

Q. And you consider yourself an activist, correct?

A. I'm an activist and a scholar and a researcher.

Q. Okay. I'm going to show you what I've marked as Government's Exhibit 1.

THE COURT: Ms. Yusi, I'm going to keep going until the government testifies, so everybody just be prepared to stay late.

MS. YUSI: Thank you, Your Honor.

BY MS. YUSI:

Q. Do you recognize this?

A. Yes, ma'am.

Q. What is it?

A. These appear to be printouts of tweets of mine from Twitter.

Q. And what is Twitter?

A. Twitter is a social network.

Q. Okay. And you have an account there?

A. Yes, ma'am.

Q. And you frequently tweet about personal and professional observations?

A. It's mainly professional.

Q. Mainly professional.

A. Uh-huh.

Q. This is the front page of your Twitter account, correct?

A. That is my Twitter home page, yes, ma'am.

Q. And how do you describe yourself?

A. In my bio it says I fight surveillance, and then it says, "Views expressed here are my own," which, as I described before, my employer asked me to put.

And then -- do you want me to continue?

Q. No, that's okay.

And I'm going to show you page 2 --

MS. YUSI: I'm sorry, Your Honor. The government moves to admit Exhibit 1.

THE COURT: You're going to have to speak into the microphone.

MS. YUSI: I'm sorry, Your Honor.

The government moves to admit Exhibit 1.

THE COURT: This is merely for what purpose, ma'am?

MS. YUSI: Your Honor, bias, to show the expert's --

THE COURT: Has he admitted to this?

MS. YUSI: He admitted that these are tweets that he wrote on his Twitter account.

THE COURT: All right. It's admitted, but I haven't looked at it yet, other than the front page of this thing.

MS. YUSI: I'll go through it, Your Honor.

THE COURT: Okay.

(The exhibit was admitted into evidence.)

BY MS. YUSI:

Q. Page 2. Is this one of your tweets?

A. Yes, ma'am.

Q. And what did you say?

A. Are you asking me to read it, or --

Q. I am asking you to read it.

A. So this is a tweet @daveaitele, who is an ex-NSA analyst.

"The FBI shat the bed with their Playpen op. An overbroad, illegal warrant, and no chain of custody for the data they collected."

Q. At this point had you looked at things on some of these defendants' computers?

A. I've never looked at any defendant's computer, ma'am.

Q. I'm talking about the information that was sent. Had you looked at the NIT and the source code and the affidavit or the search warrant? At this point had you looked at those?

A. What is the date of this tweet?

Q. I'm not sure. You remember writing it, though, so --

A. That's because I was shown it in court last week.

Q. Okay. And at that point you said you didn't remember, right?

A. I didn't remember if I had tweeted it, but then one of your colleagues from the U.S. Attorney's Office in Arkansas showed me a printout, and I believe I said, "That looks about right."

Q. Okay. And do you remember the date?

A. No.

Q. So you're not sure if you had this opinion before or after you started testifying?

A. Testifying or looking at stuff?

Q. Either.

A. Well, I testified in the *Michaud* case, which was the first one, but never looked at the NIT or the PCAP file. I never looked at any of the evidence that was under protective order in that case. I only looked at that in the Arkansas case, in which I testified two weeks ago.

Q. But you have an opinion that everything that the FBI did in this case, or the NIT, was illegal, correct?

A. I have a personal opinion that the method that the government employed exceeded Rule 41 of the Rules of Criminal Procedure and that it has some serious Fourth Amendment issues to it, yes, ma'am.

Q. Okay. And you want to see the source of all this in order to further show that you believe it's illegal, correct?

A. No. I believe that the legal issues can -- the Rule 41 issue I believe doesn't involve the source code. I believe that the Fourth Amendment issue as to whether searching 10,000 or 50,000 computers with a single warrant -- whether that -- I don't think the code is important there.

I think in this case, you know, if you -- there are things that the defense counsel, I think, wants to be able to see, such as the chain of custody, such as the state that the computer was in before it was hacked, the state the computer was in after it was hacked, where the code would be useful.

I'm actually, as I -- I assume you've read the Arkansas transcript. As I said there, I'm actually not the right person to look at the exploit itself. I don't want to look at the exploit. I don't have the skills for it. In the same way you wouldn't hire a tax attorney to do a murder defense, I don't have the specialized skills to look at the exploit.

Q. So you want to be -- just to be clear about your position just in general, you want to fight surveillance and limit the government's ability to surveil on the Internet, including Tor?

A. I believe in the Fourth Amendment, and the Fourth Amendment limits the role of government, and the Fourth Amendment creates a role that judges have to play of supervising surveillance tools, and I think that it would be a really awesome thing if the Fourth Amendment more robustly were applied to the use of NITs.

Q. So the Fourth Amendment was violated in this case, and you believe that without even having seen what you call the whole NIT in this case.

A. So, as I said before, in my view there are real questions about whether a single warrant can be used to authorize 50,000 or 100,000 searches.

THE COURT: Were there 50,000 users of this child pornography site? Is that what you're saying?

THE WITNESS: The FBI has testified that there were 100,000 people who visited the site in the two weeks that it was under the government's control, but they have not revealed how many of those were --

THE COURT: 100,000?

THE WITNESS: Yes, Your Honor, but they have not revealed how many of those the NIT successfully operated against.

THE COURT: 100,000?

BY MS. YUSI:

Q. And if there were 100,000 people, you agree that law enforcement still has an obligation to try to investigate who is a part of this Web site, correct?

A. Sure.

Q. And regardless of how many there are, if it's a legal warrant then it's a legal warrant, correct?

A. No. I think that -- I think that the Fourth Amendment -- the Fourth Amendment should not permit searches of such a huge scope. I think that if -- with a single warrant the government can search thousands of computers --

Q. But this personal opinion -- I mean, you have this opinion, and you're applying it to see the -- you want the NIT released, correct, in an effort to further your personal opinion.

A. I don't know that anyone is asking for it to be released, ma'am.

Q. You're asking for access to it, and that's to further your personal opinion, correct?

A. I haven't asked for access to the NIT for my sake, because I don't have the skills to look at the exploit. The NIT has already been turned over to the defense.

Q. Okay.

A. The exploit is something that I don't have the skills to analyze.

Q. But you're opining as to why it would be important.

A. Sure, but whoever will look at that will be under a protective order, just like I'm under a protective order for the NIT.

Q. And you also criticize the FBI publicly on a regular basis. Is that right?

A. As I also criticize companies and other parts of the government, yes, ma'am.

Q. Let me show you page 3 of Exhibit 1.

And you're criticizing the FBI for saying that they can't be bothered to use security, a secure Web site, correct?

A. Yes, ma'am. Would you like me to describe that?

Q. No.

A. Can I?

Q. I haven't asked that question, but --

A. Well, may I describe what I'm saying here?

Q. Sure.

A. Okay. Last year the Office of Management and Budget required every federal agency to encrypt their Web sites. By default, the FBI home page is now encrypted, as are many U.S. Government agencies.

Over the last few months and the last year, I have pushed different parts of the government to follow that order, and I have had personal conversations with the FBI's general counsel about encrypting their e-mails, for example, and they say that they're working on that. They're making slow progress, and I think that, just as the FBI has encrypted its home page, they should be using encryption on their NIT server.

Q. Let me show you what's been marked as --

A. Ma'am, there are no page numbers on this, so --

Q. Right. That's why I'm counting. Page 6, where it starts with, "The FBI's malware transmits data back to the FBI server." And it will be on your screen, too.

A. Okay.

Q. Do you see that?

A. Yes, ma'am.

Q. So, again, you're commenting on the FBI, and what does "face palm" mean at the end?

A. "Face palm" is a way of expressing shock at an action.

Q. That means -- okay. So you're, once again, commenting on --

A. So this is -- embedded under that tweet is a screenshot from -- wait a minute. I haven't seen this in a while.

(There was a pause in the proceedings.)

BY MS. YUSI:

Q. You're commenting on the Matish case here, correct?

A. That's correct.

Q. And that's the other case in this court in front of Judge Morgan. Is that correct?

A. This would have been a public document, and I was embedding a screenshot from a public document and summarizing for a lay audience what that document said.

Q. So you're advertising what you're doing on your behalf in your pro bono as an expert, correct?

A. No, I'm describing facts that have come to light in public proceedings.

Q. Okay. And you're also bragging about providing declarations and things like that in these cases, correct?

A. What do you mean by --

Q. I'm going to show you -- you can look on the screen, too.

"I wrote an 8-page expert declaration in an FBI hacking case." And you --

A. I don't see anything there that's bragging.

Q. If you can look on the screen --

A. No, I see the tweet. I'm saying I don't see that as bragging. I'm publishing a link to a copy of a declaration that I downloaded from PACER, which is a publicly accessible system. I paid for the declaration through PACER and published it because there are a number of scholars, academic scholars, and journalists who are really interested in NIT-related issues.

Q. Okay. And this is your livelihood, correct? I mean, you want to continue this livelihood after this case is over, correct?

A. So the way it works at the ACLU is I'm actually not told what to work on. So no one said, "Chris, please spend time on NITs."

I think this is interesting, so I chose to work on this. There are a million other issues I could work on. There's no shortage of interesting Fourth Amendment issues, and so if the entire NIT issue went away I would move on to body cams or GPS darts or whatever new surveillance technology the government uses. There are plenty of people who want to learn how they work and have me explain it to them.

Q. Okay. And, as you said, you fight surveillance, and particularly government surveillance is what your main focus is.

A. I mean, I worked in consumer privacy issues for a few years, but I've shifted my work towards government issues, yes, ma'am, the U.S. Government but also other governments.

Q. I want to talk to you about your declaration and some of the things you were testifying about earlier.

A. Sure.

Q. Do you have a copy of your declaration?

A. I don't. Do you have a spare copy that you could give me?

Q. Yes.

(There was a pause in the proceedings.)

BY MS. YUSI:

Q. I'm going to show you what we marked as Government Exhibit 2.

MS. YUSI: Your Honor, this is just a copy of -- I don't know if I need to admit it into evidence, but I will do so now, the declaration of Dr. Soghoian, just for ease sake.

THE COURT: Was it attached to --

MS. YUSI: It was attached to the reply in support of Defendant Eure's motion to compel.

THE COURT: Okay.

(The exhibit was admitted into evidence.)

BY MS. YUSI:

Q. If we could look at paragraph 19 on page 5.

A. Yes, ma'am.

Q. And that's where you're criticizing the FBI about not using encryption for information that was transmitted by the NIT to the FBI server, correct?

A. Yes, ma'am, that's true.

Q. Now, when you talk about how someone could possibly have tampered with that information, that's speculation, correct?

A. Sure.

Q. Okay. There's no proof of any of that in this particular case, correct?

A. It is very difficult to detect tampering with unencrypted data as it goes over the Internet.

Q. So it's just speculation that you might be able to see something when you looked at it, correct?

A. When you say "you" do you mean me, or do you mean someone watching the data as it's going over the network?

Q. I'm talking about you looking at the exploit or the unique identifier that you want to look at.

A. The unique identifier and the exploit have nothing to do with encryption issues.

Q. Okay. All right. So --

A. The encryption issue is about chain of custody --

Q. Okay.

A. The exploit is about the state of the computer and whether the information derived from it was forensically sound.

Q. Okay. How would it work? Do you know how it would work if someone had -- what would have to happen if someone was to have changed the information that was sent from the user back to the FBI?

A. Sure, I can explain that. So when data is sent over the Internet it goes from your computer to a remote server, say the FBI's Web site, and it has to -- we don't have direct connections, direct lines, from, you know, our houses to every Web site we visit. We have to go through a bunch of points along the way, and those points are servers or devices that are called routers that are run by companies like Comcast, Verizon, and AT&T. And at every point along the path anyone controlling that server, either the operator of the network or a hacker or a foreign government that has gained improper access to those devices --

Q. Are you saying that a foreign government is involved with hacking this particular case?

A. I don't know, but I -- would you like me to finish what I'm saying, or --

Q. No, I'm just -- you're saying a lot, so I'm trying to --

A. Governments hack routers. This is a known thing. The U.S. Government hacks foreign communications networks, and I'm sure that China and Russia hack U.S. Government networks. This is why there are a lot of people working in cyber security these days.

Generally, servers that deliver our data are not trusted anymore. This is why large responsible organizations now use encryption to protect data. This is --

Q. And I get that, but what I'm asking for is the NIT was sent to a user's computer, correct? And then that NIT got the information from that computer and sent it to the FBI immediately, correct?

A. I mean, there might have been a one-second delay, I don't know, but quickly.

Q. Someone, if it was unencrypted, would have to hack it or be involved with it during that one second, correct?

A. No.

Q. No?

A. No.

Q. Okay. So --

A. If they had already hacked the server and they had --

Q. Hacked the FBI's server?

A. No, ma'am, hacked one of the servers or routers sitting between an individual NIT user and the government server. Either someone who has hacked it, an employee or a piece of malfunctioning software on one of those computers, could change data that is going through it, just as the government's own server changed the IP address in the PCAP file that you gave to me.

Q. Okay. Well, the PCAP -- let's talk about that.

You're talking about something that was -- you're talking about the review of the PCAP data indicated that the -- seized from the defendant's computer changed in transit, correct?

A. Uh-huh.

Q. When you're talking about that, are you talking about the substantive data or the header that was sent back?

A. The IP address appears in the header, not the -- if you have, like, the envelope and the data that's inside the envelope, it would be the data on the outside of the envelope that was changed.

Q. So it's like the header of an e-mail. Like when you reply to something you don't change the subject, but it says "Re," R-E. When you reply to most e-mails accounts it automatically does that on the header, correct?

A. I don't think that's a great analogy. I think -- I mean, there are other ones that I --

Q. I'm just saying it's the automatic change of a header as it goes through.

A. Certainly, the two changes that definitely occurred here were automatic. We have no way of knowing if there were any other changes, because you didn't use encryption.

Q. So when you're telling the Court that you found indications that something was tampered with, you were talking about automatic changes.

A. I'm saying that the data in the PCAP file is not the same information that left the defendant's computer.

Q. Because of automatic changes in the header.

A. So it was changed probably by the Wi-Fi router in the defendant's home, and that would have been a change of the source address. And then whatever government server was --

Q. I'm asking -- it was automatic, correct?

A. Yes.

Q. And you want the Court -- you were trying to have the -- your information to the Court was automatic changes mean that that's evidence that there could be other changes in the substantive. Did you find any changes in the substantive?

A. No. This is the -- the IP address isn't in the substantive part, the IP address appears in the header.

Q. I'm talking about the substantive portion. You found nothing different in that from what was sent to the user to what was sent back to the FBI.

A. We don't know what --

Q. You looked at the PCAP.

A. Right. That only shows what was received by the FBI.

Q. Okay.

A. It doesn't show what left the user's computer.

Q. You saw the unique identifier in both what was sent to the computer and what was received by the FBI. Is that right?

A. I saw the unique identifier that was received by the PCAP -- that is contained in the PCAP file.

Q. So just to be clear, there are no substantive changes. You saw automatic changes, and that is what you're relying on to say that there's a possibility that there were other changes.

A. I think that's not a great way of saying it. You didn't give me --

Q. Is that a simple way to say it?

A. No. You didn't give me two PCAP files. It's not like I looked at one file and looked at another and saw something change from A to know B. All you gave me was one file, but I can tell from the IP addresses that are in it that it was changed twice.

Q. And wasn't it a two-way communication file?

A. That's what the government called it, yes, ma'am.

Q. And then what was sent to the computer, the computer instructions, you were also given that, correct?

A. We don't have a PCAP file of the instructions being sent. We don't have a --

Q. But you actually have the source code that was sent there.

A. No, we don't have the source code, we have the computer code, the object code.

Q. I'm sorry, the object code. You have that of exactly what was sent there.

A. Yes, but that's not -- that's the code that gets to the computer. What's missing is the exploit, and then what's missing is a PCAP file saved from the defendant's computer.

Q. And you were also speculating as to looking at a defendant's computer may not be helpful, correct?

A. I answered some questions about that.

Q. Okay. But you said it would not be helpful.

A. I said over time it would be less and less helpful.

Q. Okay. But you don't know that for sure, so you're speculating.

A. I mean, when you reboot a computer, whatever is in memory disappears. And, so, if you --

Q. That's in the ram, not in your hard drive.

A. That's correct.

Q. And ram is very small in most computers, correct?

A. I mean, we generally have much less ram than storage space, yes, ma'am.

Q. And most of the things that are found on computers are going to be in your external hard drive, and that, if it's done correctly by a trained forensic person, is going to be the exact same as when that computer was turned off.

A. So the data that the NIT collected, such as the MAC address, that's not stored on the hard drive. That's stored initially in the Wi-Fi card, but it can be changed by running software, and then that would be in memory.

Q. And in this particular case you looked at at least Mr. Eure's information from his computer, correct?

A. I haven't looked at information from his computer, no, ma'am.

Q. Okay. So let's say hypothetically that the MAC address was -- the exact same MAC address that was sent to the FBI was the MAC address of Mr. Eure's computer that contained child pornography.

Would that change your speculation as to whether or not you need an exploit to prove any infirmities?

A. No. So, as I said before, having the exploit will give you some indication as to whether the computer was left in either a secure state or an insecure state, and without the exploit you don't know if information that's on the computer -- that's stored on the computer was downloaded by the defendant or may have been put there later by someone else.

Q. How about a defendant -- hypothetically, let's say both defendants, Mr. Eure and Mr. Darby, in this case, confessed that they used Playpen, that they had those exact user names that were in their search warrants, and that they were responsible for what was on their computer and what they saw in Playpen.

Would that change your opinion that the exploit and the unique identifier generator is necessary?

A. That they -- so I need to ask a clarifying question of you.

Did they say that every single file that was on the computer was downloaded by them?

Q. This is a hypothetical --

THE COURT: They didn't say every single file was anything. They just said the information contained on the computer was their information on their computer. And the fact that that information was what the FBI had also discovered makes no difference to you, does it?

THE WITNESS: If -- knowing -- being able to see the exploit -- and, to be clear, not me but someone skilled in the art of malware and exploit analysis being able to look at the exploit --

THE COURT: The question is it doesn't make any difference, because isn't it true that you challenge all computers where they don't use encryption; that is, that includes all e-mail providers, social networking sites, and any Web sites that transmit computer data. Is that correct?

THE WITNESS: I'm sorry, sir, I don't understand the question. Can you ask it again?

THE COURT: Let me say this:

You challenge all of the companies that are not using an encryption by default. Isn't that correct?

THE WITNESS: I have spent several years pushing companies and government agencies to encrypt their data, yes, sir.

THE COURT: I didn't ask you about several years, I asked you is it true -- and I'll repeat it -- "I challenge all the companies that are not using https by default."

Is that correct?

THE WITNESS: Challenge to what? What are you reading from?

THE COURT: "...includes all e-mail providers, social networking sites, and any Web site that transmits consumer data. Step up and protect consumers. Don't do it just some of the time, make your Web sites secure by default."

THE WITNESS: Okay, now I know what you're quoting. That's a statement by Pamela Jones Harper, a Commissioner at the Federal Trade Commission. Those are not my words, those are hers.

THE COURT: So you don't agree with it.

THE WITNESS: I agree with it.

THE COURT: You printed it.

THE WITNESS: I think I cited it.

THE COURT: Yes, and you gave it verbatim in your declaration, did you not?

THE WITNESS: Sir, that's a quote in a footnote.

THE COURT: I understand.

THE WITNESS: Okay.

THE COURT: But you gave it. I didn't dream it out of the air, did I?

THE WITNESS: You didn't dream it out of the air, but --

THE COURT: Okay. You know, you're going to have to start answering questions and stop arguing all the time about every question. Nobody is trying to trick you in any way, we're just trying to get at what you're seeking to achieve.

You're seeking to achieve the fact that the FBI did not encrypt the material it was sending back, correct?

THE WITNESS: Yes, Your Honor.

THE COURT: And that's it in a nutshell, isn't it?

THE WITNESS: I believe that the government should have encrypted the data, because it would have provided tampered evidence.

THE COURT: That's all right. Okay. Let's move along, Ms. Yusi.

BY MS. YUSI:

Q. Now, you did agree -- just to touch base with the suppression issue, you agree that every user and every person that's been charged, or has allegedly been involved with Playpen and charged, that that person had to choose to go to the Playpen site, correct?

A. I don't believe I said that.

Q. You said everyone that got the NIT had to go to the Playpen Web site.

A. Right, but I didn't say that they had to choose to go. So it's possible to visit the site without choosing to go there.

Q. Okay. Let's say they open up an account and they've been seen well before the NIT, they continue to use the site; they use it afterwards, too. Okay? Let's say that. They go to -- they're choosing to go to a Web site at that point, correct?

A. Sure.

Q. And they have to go to the Eastern District of Virginia to get information from that Web site. Do you agree?

A. No, they don't go into the Eastern District of Virginia.

Q. They cause their computer to go into the Eastern District of Virginia, or the Internet, or whatever --

A. When I call my family in New Haven I'm not entering the City of New Haven, I'm sitting in Washington, D.C. making a telephone call. And my voice is turned into digital data, and it goes over a phone line, but I never leave D.C.

Q. You also talked about what the FBI knew in terms of activity of each user on the Web site, correct?

A. Yes, ma'am.

Q. You said you don't know what they knew, if they knew anything. Is that right?

A. Well, so, we've seen in several cases the government has described information in affidavits about how many hours individuals spent logged in to the forums, when they created their accounts. So there's certainly some information that was collected and created initially by the server administrators and then further supplemented by the government.

Q. And there's activity logs or user reports?

A. Yes, ma'am.

Q. And, so, the FBI knew what was going on, at least in those cases that you know about?

A. The government knew about activity associated with accounts but not with IP addresses.

Q. Right. Until there's a NIT, right?

A. Until they hacked the computers of the people visiting the site, yes, ma'am.

THE COURT: You have seven minutes left, Ms. Yusi.

MS. YUSI: Yes, sir. If I can have one moment.

(There was a pause in the proceedings.)

BY MS. YUSI:

Q. One last thing:

You said earlier that encryption is a guarantee of safety, correct?

A. Did I say that today?

Q. Yes.

A. When did I say that? Can you read that back?

Q. I don't think we need to, but -- okay. So you agree that encryption is not a guarantee?

A. That's correct. Encryption -- just like a doctor washing his or her hands before surgery is not a guarantee that you'll come out of surgery in good condition. If they don't wash their hands, you're going to have a really bad time, and encrypting is a contributing element to good cyber security hygiene.

MS. YUSI: Thank you. Those are all my questions, Your Honor.

THE COURT: Any other questions?

MR. GRINDROD: No, Your Honor.

THE COURT: Thank you very much, sir. You may step down.

Who is your next witness?

MR. GRINDROD: Your Honor, there are no further defense witnesses. We would just offer the transcript from proceedings before Judge Morgan in the United States against

Edward Joseph Matish. The parties have reached an agreement that we will submit this transcript for the Court's consideration with respect to the pending motion to suppress in Mr. Eure's case.

THE COURT: The entire transcript from Judge Morgan's case you want to admit?

MR. GRINDROD: Yes, Your Honor.

MS. YUSI: And, Your Honor, I have no objection, but I do want to say I agreed to this not knowing that we were going to rehash the majority of things for the last two hours. But that's fine, if we still need to do that.

THE COURT: Well, we'll just keep going, because I'm going to finish tonight. So don't plan on going anywhere.

MR. GRINDROD: Yes, sir, Your Honor. If I could submit this for the Court.

THE COURT: All right.

MR. GRINDROD: It's been marked as Defendant's Exhibit 1.

(The exhibit was admitted into evidence.)

THE COURT: I've read Judge Morgan's opinion, which is a very interesting opinion, and it differs somewhat from my prior opinion. So where are we going? This is admitted to show what Judge Morgan's opinion is about, and he ruled against your position.

MR. GRINDROD: That's correct, Your Honor. We're certainly not submitting it for the same outcome in that case, but we called Agents McFarland and Alfin in that case to testify, and in order to not just duplicate that testimony we thought it would be more efficient to submit their testimony.

THE COURT: So all of your testimony is in here.

MR. GRINDROD: Yes, sir, that's the full transcript, including argument. But, I mean, I don't think the argument is necessarily relevant to the --

THE COURT: Well, that's what this case has been about, was the whole argument instead of the testimony of a witness. And I don't like it if it's not testimony. I tell you, try to stick to testimony from everyone. It's not any one person.

Okay. What else have you got, Ms. Yusi?

Have you got anything else?

MR. GRINDROD: No, Your Honor.

THE COURT: All right. All right, Ms. Yusi.

MS. YUSI: Your Honor, I'd like to call Special Agent Alfin. And the transcript, that's regarding the motion to suppress. I'm going to be very brief and just kind of address some of the issues that Dr. Soghoian went into with Special Agent Alfin.

THE COURT: Well, let's take a break right now. Let's take a 12-minute break by that clock.

MS. YUSI: Yes, sir.

(A recess was taken.)

THE COURT: All right, Ms. Yusi.

MS. YUSI: Thank you. Your Honor, we call Special Agent Alfin from the FBI.

(The clerk administered the oath.)

DANIEL ALFIN, called as a witness, having been first duly sworn, testified as follows:

DIRECT EXAMINATION

BY MS. YUSI:

Q. Could you introduce yourself, Special Agent Alfin, to the Court?

A. My name is Daniel Alfin, last name spelled A-L-F-I-N. I am a Special Agent with the FBI. I'm currently assigned to FBI Headquarters, Criminal Investigative Division, Violent Crimes Against Children Section, Major Case Coordination Unit, located in Lithicum, Maryland.

Q. And how long have you been an FBI agent?

A. I've been employed as an FBI agent since 2009.

Q. And in your current position what sort of cases do you work on?

A. My role at the Major Case Coordination Unit is to investigate individuals who use various types of technology to facilitate the production, trade, and distribution of child pornography. Specifically, my investigations involve individuals who use the Tor network.

Q. Are you the case agent for the national Playpen investigation?

A. I am.

Q. And when did you start being involved with the investigation of Playpen?

A. I became aware of Playpen shortly after it came online in approximately August, 2014.

In December, 2014, the FBI learned the true location of the Playpen Web site, and we initiated an investigation. I have been involved in that investigation from the beginning.

Q. Okay. And you've submitted a declaration in this case and others concerning the NIT that was involved in the investigation?

A. I have.

Q. All right. And I'm going to talk to you just briefly about or ask you questions about certain points. You were here when Dr. Soghoian testified, correct?

A. I was.

Q. All right. He talked about encryption and the possibility of someone tampering with the information that came from the user to the FBI servers. Can you talk about -- well, the FBI did not use encryption, correct?

A. That is correct, the information transmitted by the NIT was not encrypted.

Referring to Dr. Soghoian's testimony, in theory he is correct. Generally, data that is not sent in an encrypted format can be tampered with. That is a theoretical possibility; however, it is not an issue in the matter at hand for a number of reasons. Despite the fact that the data that we sent was unencrypted, a number of things would have had to have taken place in order for someone to tamper with it.

First of all, an individual would have had to have known about the FBI's operation. They would have had to have known sensitive government information about the FBI takeover of a Playpen Web site. They would have had to have known that we were deploying a NIT on the Web site to identify users. They would have had to have known how the NIT functioned and how it sent data back to the FBI.

Additionally, a user would have had to have known information from the defendant's computer. They would have had to have known the unique identifier on the defendant's computer, previously referred to as a MAC address, among other pieces of information. They would have had to have known that the defendant was a member of the Playpen Web site.

In addition to all of this, an attacker would have had to have the capability to intercept the data from the defendant's computer to the government. There is no person or organization that could have known or had the capability to do all of these things, and so I can say with certainty that the data that was collected by the government in this operation is true and accurate.

Q. Now, I'd like to talk to you about what has been made available to the defendant.

Could you describe the two things that have been made available to the defendant?

A. A number of things have been made available to the defendant. All of these things are the necessary pieces of information that would be needed to prove what has been referred to as a digital chain of custody.

First of all, we have made available to defense for review the NIT that seized the data from the defendant's computer. We have also made available to defense the defendant's computer itself from which that data was seized.

Additionally, we have made available to defense the network data that was captured by the government, showing the data that the NIT sent to the government from the defendant's computer.

These three things on their own can prove the digital chain of custody, showing that the data originating from the defendant's computer was, in fact, what was collected by the government and what was, in fact, used in its investigation of the defendants.

A fourth piece of information that further emphasizes the fact that the data collected was accurate is the fact that the defendants admitted to the activity on the Playpen Web site of which they were accused. The primary purpose of the NIT was to associate a user account on Playpen with a real-world person. In both instances at hand both defendants admitted to that activity, so that further throws out any concern of alleged digital chain of custody issues.

Q. Do you know if either of the defendants have requested that a forensic person or someone else, another expert, look at the computers that were seized from their house?

A. It is my understanding that the digital devices seized from the residences of the defendants have been made available to defense for review; however, defense has not made any attempts to review or analyze those devices.

Q. Now, in order to also, I guess, test your theory -- or not your theory but what the FBI said, the information that matches the computer back to what the FBI received, did you do any tests, or are there any tests available to do that?

A. Yes. In order to validate that the information that the government received and provided the defense is accurate, you would need to analyze a number of pieces of information, all of which I described previously, all of which are available for defense to review, including the defendants' computers, the network data stream, the actual NIT, and the statements made by the defendants.

Q. And with that information can they -- what can they do with it in a sterile environment, I guess, to test it?

A. All that information that has been provided to defense can be used to confirm that the evidence used in the charges at hand were -- that that evidence was good and accurate.

Additionally, the NIT source code that has been provided to defense can confirm that the information that the NIT was authorized to collect is the same as the information that the NIT did, in fact, collect and that it did not collect anything outside the scope of the warrants that authorized its use.

Q. Dr. Soghoian also talked about "unique identifier generator." Did you hear that testimony?

A. I did.

Q. And can you expound on what he said?

A. When the NIT is downloaded to a user's computer it includes a unique identifier. Every identifier generated during this operation was, in fact, unique. I know this because as the case agent I have access to every single unique identifier that was generated in this investigation.

I have reviewed every single unique identifier in this investigation in order to determine that there were, in fact, no unique identifiers generated more than once.

Q. If you had found a duplicate unique identifier, what would you have done with that information?

A. If a unique duplicate identifier had been found, I would have attempted to identify the source of that duplication; however, there were no unique identifiers generated, so it's not an issue that I had to deal with.

Q. Okay.

MS. YUSI: Your Honor, I think those are all of my questions at this time.

THE COURT: Mr. Grindrod.

MR. GRINDROD: Thank you, Your Honor.

CROSS-EXAMINATION

BY MR. GRINDROD:

Q. Let's pick up where Ms. Yusi left off. You were talking about the unique identifier or the creation of unique identifiers.

A. Yes.

Q. And you talked about a list of unique identifiers that you reviewed.

A. Yes.

Q. Was that the list of the unique identifiers that were sent out by the FBI or the list of unique identifiers that were successfully returned to the FBI?

A. It was the list of unique identifiers that were generated by the FBI. So "sent out by the FBI," I think that would be an accurate description.

Q. And you reviewed that list and compared, what, each unique identifier to every other identifier?

A. It's a very simple process. You put every unique identifier in a spreadsheet, and you say "find duplicates" and the spreadsheet says there are no duplicates. It's very simple to do.

Q. Have you produced that spreadsheet to the defense?

A. No. I have provided the unique identifier used in the matter at hand.

Q. And even if you're not providing the code that created the unique identifier, to your knowledge, has the government produced any indication as to how that unique identifier was even created?

A. Yes, we generated unique identifiers.

Q. Using an algorithm?

A. Yes.

Q. Did you write that algorithm?

A. I did not.

Q. Do you know that algorithm?

A. I do not.

Q. Would you recognize it if you were presented with it?

A. I would not.

Q. Can you explain the inner workings of how that algorithm works?

A. I can. It generates a unique identifier.

Q. That's the inner workings, as far as your understanding goes?

A. Could you be more specific in what you're asking for?

Q. Well, this unique identifier is a piece of computer code, correct?

A. No, it's a string of text.

Q. It's a string of text?

A. A unique identifier is a string of text, yes.

Q. It's a generator. It's computer code.

A. The generator could be described as computer code, yes.

Q. And it runs on a system.

A. Yes.

Q. What system does it run on?

A. A government-controlled computer.

Q. Okay. And is it operated inside any -- is it just operating in some program that is unique that is created by the government in order to create these unique identifiers? Does it run within Excel? You mentioned that there may be spreadsheets involved.

I'm trying to figure out how, from a technological perspective, this generator worked.

A. When a NIT is packaged or put together it generates a unique identifier, and it injects it into the package that is downloaded to the user's computer.

Q. Okay. And that's what it does, but now my question is how does it do that?

So this creation of a unique identifier, you said that that is created through some sort of computer code. What I'm trying to figure out is how exactly, from a technological perspective, is the unique identifier created?

MS. YUSI: Your Honor, I'm going to object.

THE COURT: We're going into the code itself. Isn't that where we're going?

MR. GRINDROD: Your Honor, in the event the government is not going to produce it, perhaps Agent Alfin can explain how the code works so that we can understand why there is some alleged law enforcement privilege that covers it.

MS. YUSI: Your Honor, if I may interject, I don't think any of these other unique identifiers are important. The only ones that are important are the ones that went to the two defendants.

THE COURT: Well, there isn't any question the -- there is testimony that an IP, I believe, was different from one sent that one existed, and I thought we would probably be going into that some day.

MS. YUSI: That's a separate issue, Your Honor.

THE COURT: Well, I'm not going into the code. I can tell you that. And we're not going into the code, so --

at this time. We may go into the code later, but it's only after I make a ruling on whether the code is discoverable or not. So we're not going into it at this time. We're knowing that the code was utilized, and that's all that I'm going into or all I'm going to allow at this particular portion. So let's don't go into what the code is or does and how it works, because that's one way that it could be released. The problem about codes that invade Tor is what it may lead to.

We have tremendous security problems at the present time with encrypted materials being utilized by those people whose main object in the makeup of things at the present time is to kill nonbelievers, and unfortunately there are a great many nonbelievers right in this room at this time. And so, therefore, they are everywhere. And since there is an organization who would love to get into Tor to find out what the government is doing, I'm not about to release anything unless it's essential, and then the government would have to decide whether it's going forward or not with the case.

MR. GRINDROD: I understand, Your Honor.

THE COURT: But I'm not going to go into it on examination of this witness.

BY MR. GRINDROD:

Q. Agent Alfin, without providing any further explanation than what you've already provided, can you just tell me whether you have -- you personally could give any more detailed explanation about how the code worked than what you've already provided here in court?

A. Which specific code?

Q. The unique identifier generator. Just a "yes" or "no." I don't want to get into any --

THE COURT: Unique identifier -- which one are you speaking of, the one that found Tor or the one that found the defendant?

MR. GRINDROD: I think Your Honor may be referring to the IP address.

THE COURT: Yes.

MR. GRINDROD: And I'm referring, instead, to the FBI-generated code that was injected into the packet of information that was sent from our clients' computers to the FBI as a means of linking up the Playpen use with the user account. This was a number that the FBI created in order to uniquely identify people, and what I'm trying to figure out is whether Agent Alfin even has an understanding as to how that code worked.

THE COURT: I'll allow that.

BY MR. GRINDROD:

Q. So, Agent Alfin, I'll ask you again. Again, without providing a substantive answer as to how the code may or may not have worked, do you have the ability to provide any more detail as to how the unique identifier generator worked in this case from a technological perspective?

A. I've already explained in detail how it works from a technological perspective, so I would still need you to clarify what exactly you're asking, because your questions don't make sense from a technical standpoint.

Q. So, as far as you're concerned, everything about how it works has been said.

THE COURT: I don't know about everything, but --

THE WITNESS: I have not --

THE COURT: Where has it been said?

THE WITNESS: The actual mathematical algorithm that generates the unique identifiers, that has not been stated. I do not know that mathematical algorithm.

BY MR. GRINDROD:

Q. Or how it was created?

A. How the mathematical algorithm was created?

Q. What went into its design? Presumably, the point of the algorithm is to ensure it produces unique numbers.

THE COURT: I'm not going into how --

MR. GRINDROD: I'll move on, Your Honor.

THE COURT: -- it was created, because that will imply a knowledge of how to get it.

MR. GRINDROD: I'll move on, Your Honor.

THE COURT: I'm not going to get into that, unless I find that the motion to produce or the motion to compel or the motion to suppress is merited. First I'd have to find that, and then you can go into it, but you're not going into it indirectly, okay?

MR. GRINDROD: Understood, Your Honor.

BY MR. GRINDROD:

Q. Agent Alfin, you've obviously prepared a declaration in this case and now testified, so I want to talk a little bit about your credentials.

Your declaration states that you hold a university degree in information technology. Can you tell me what that's in reference to?

A. I have a Bachelor's degree in information technology.

Q. And where is that from?

A. Florida State University.

Q. And did your training in information technology include computer science courses?

A. Yes.

Q. And do you have a working ability to write computer code?

A. Basic computer code, yes.

Q. But it's fair to say you're not capable of writing, for example, the NIT in this case.

A. The NIT is actually very simple computer code.

Q. Did you help write it?

A. I did not.

Q. Could you write a NIT?

A. The NIT that was used in this case? Yes, I do have the capabilities to write a NIT similar to this one.

Q. Okay. And the NIT was produced in this case, right?

A. It was.

Q. Let's talk about the exploit, then.

Do you have the technical capability to write an exploit?

A. I do not.

Q. Did you work at all in the creation of the exploit in this case?

A. I did not.

Q. You've obviously testified, both here and in your declaration, about what the exploit does and doesn't do, correct?

A. Yes, I have.

Q. Is that based on your review of the exploit?

A. It is based on my use of the exploit.

Q. Okay. And you make that clarification because you've never actually reviewed the exploit, correct?

A. Are you referring to the source code of the exploit?

Q. Well, have you looked at the source code of the exploit?

A. I have not.

Q. Have you looked at any other aspect of the exploit?

A. Such as...

Q. Such as -- so the --

THE COURT: The exploit is the code.

MR. GRINDROD: Well, that's where it gets tricky, Your Honor. I think there are various things that can be referred to as "the code" in this case, but the exploit is a code, that's correct.

So the source code --

THE COURT: What was the exploit in this case, I understood, was the code utilized in this case. So there's another exploit besides the code that was used in this case?

MR. GRINDROD: Well, Your Honor, "an exploit" can describe --

THE COURT: I know what an exploit is in this case; it's the code utilized in this case.

MR. GRINDROD: Correct.

THE COURT: And that's what's referred to in various declarations and in various testimony. Now we've got a different exploit?

MR. GRINDROD: No, Your Honor, but there are different -- so the NIT computer code is sometimes referred to as a code. That's a separate thing.

THE COURT: I understand the NIT is one thing.

MR. GRINDROD: Right.

THE COURT: The exploit was the code utilized to determine the defendant's computer, correct?

MR. GRINDROD: To determine -- no -- well, I don't think so, Your Honor. I think the exploit was what was used to hack into our client's computer. The NIT is what was used to actually collect the data and send it back to the FBI.

I think Dr. Soghoian referred to the exploit as the picking of the lock or the exploit as the drugged piece of meat that the guard dogs eat. It's what let the government into our clients' computers.

THE COURT: All right. Let's go ahead. We've got to get into it some day.

BY MR. GRINDROD:

Q. So you've not reviewed the exploit in this case. Is that correct?

A. I have not reviewed the exploit source code in this case.

Q. And all of the statements you're making about what the exploit does and doesn't do, those statements are based on your observations of running the exploit. Is that correct?

A. In part, yes.

Q. What else are they based on?

A. Based on my conversations with other people who are knowledgeable in the matter, as stated in my declaration.

Q. Who are those people?

A. Other FBI personnel.

Q. Yeah, but what people?

A. That information is subject to law enforcement privilege.

Q. The names of the people who -- so you're basing your testimony on what you were told by other individuals, at least in part.

THE COURT: In part, okay?

BY MR. GRINDROD:

Q. Is that correct?

A. Everything substantive in my declaration is based on my own observations of my own testing. It has been further supported and backed up by other statements I've received from other individuals; however, I have tested everything with regard to the NIT's functions in my declaration.

Q. Okay. So help me understand the process. So you run the exploit, you make certain observations, and you draft this declaration. Is that what happened?

A. That's fair. That is an accurate order of events.

Q. And then at that point, after you drafted the declaration, you went to other folks in the FBI and said, "Does this look right to you?"

A. No, that's not what I said.

Q. Okay. So tell me how -- what part of this declaration --

A. There are other individuals at the FBI who obviously have reviewed the source code of the exploit. I have had conversations with those individuals --

Q. And the conversations --

A. -- several times throughout the course of this investigation, both before and after I wrote my declaration.

Q. So it's fair to say there are people who are more heavily involved in the tech side of this than you, correct?

A. In certain aspects of it, yes, that's true.

Q. Specifically with regard to the exploit, right?

A. Yes, that's true.

Q. Because you don't have the ability to create the exploit.

THE COURT: He's already testified to that three times now. Don't ask it again, please. Let's move on.

BY MR. GRINDROD:

Q. And, so, is there any way that you can be more specific as to what parts of this declaration that you submitted to the Court is based on your own personal observations versus your conversations with other people?

A. I think I've been clear on that, but if you have questions about a specific portion of my declaration, I'd be happy to answer.

Q. Okay. So let's be specific about paragraph 14. So in paragraph 14 the first sentence says, "It's theoretically possible for an exploit to make fundamental changes or alterations to a computer system or to disable its security firewall."

Is that based on your own personal knowledge?

A. Yes, it is.

Q. So it's possible for an exploit to make fundamental changes or alterations to a computer.

A. An exploit. Not the one in this case, but yes.

Q. Okay. So let's figure out what the source is for that part of your statement.

The part of your statement in which you say this exploit specifically didn't make fundamental changes, is that based on your personal observations or based on what other FBI agents have told you?

A. I tested a NIT on a computer -- or, rather, the exploit on a computer under my control. I observed that it did not open up any security holes on it, it didn't place any files on it, it didn't make it any more vulnerable to outside attackers. It is based on my observations and my testing.

Q. And how many times did you run the exploit before you reached that conclusion?

A. A few times. I don't know the exact number.

Q. More than five?

A. Possibly. Less than a hundred.

Q. Was it less than ten?

A. It may have been.

Q. Okay. Have you received any training on how to test software or computer code like an exploit?

A. I have.

Q. And where was that training?

A. I have received courses in malware analysis put on by FBI and FBI contractors.

More importantly, I have conducted analysis of such code on several occasions during the course of both criminal investigations and national security investigations. I have analyzed exploits used by criminals trying to steal money. I have analyzed exploits used by foreign countries trying to steal state secrets.

In all of these cases I have successfully found and analyzed this code without -- obviously, these foreign governments were not kind enough to give me the exploit on the front end; however, that did not stop me from being successful in my analyses.

Q. And as part of that training that you received were you taught the appropriate way to test an exploit to determine whether it creates software vulnerabilities is to run it been 5 and 10 times?

A. You can run an exploit that does one thing as many times as you want. If it's programmed to do one thing, it's going to keep doing that one thing.

Q. Okay. So my question was did you receive as part of -- you said you received training in malware analysis, and I'm asking whether as part of that training you were taught that an appropriate means of testing an exploit to determine whether it makes fundamental changes or alterations to a computer system is to run that exploit between 5 and 10 times.

A. I don't recall whether or not there was a number involved in that training. I was taught how to analyze malware.

Q. So you don't have any recollection --

THE COURT: He wasn't taught in that training. Don't argue with the witness. Let's go along and ask questions.

BY MR. GRINDROD:

Q. Was the NIT ever programmed to collect the IP address of the activating computer?

A. The NIT collects pieces of information identified in the NIT search warrant attachment and transmits it to the government. At that point we can see the IP address that data is originating from.

Q. Let me ask you my question again.

Was the NIT ever programmed to collect the IP address of the activating computer?

THE COURT: Of whose computer?

MR. GRINDROD: The activating computer, the user's computer.

THE COURT: The user's computer. Go ahead.

THE WITNESS: Your question is not technically sufficient for me to answer it "yes" or "no," and so I would have to rely on my statements, unless you can rephrase your question.

BY MR. GRINDROD:

Q. Do various forms of the NIT exist?

A. Yes. Or, rather, multiple -- every NIT used in this case was unique.

Q. And were there ever versions of the NIT that was used in this case that instead of collecting the IP address as sort of a byproduct of the other information -- was the NIT ever written in a way so that it collected the IP address from the activating computer itself?

A. Could you define what you mean by "collect" in that statement?

THE COURT: From which computer are we speaking of, now? You've got two computers that I think we're interested in. One is the computer that was transmitting Playpen, and the other was the computer utilized by the defendants or one or more of the defendants.

So we have actually three computers involved in the motion to compel, as I understand it. We may have four, because there may have been another computer transmitting information, as the other expert has testified to, a different computer transmitting the information back to the FBI than there was collecting information. So there may be four computers.

MR. GRINDROD: I'll try to be more specific as to the computer.

THE COURT: All right.

BY MR. GRINDROD:

Q. So, Agent Alfin, when I use the term "activating computer" or "the user's computer" I'm talking about the defendant's -- the to-be-defendant's computer, the computer that was the target of this search. Do you understand that?

A. Yes.

Q. Okay. So my question was whether the NIT -- whether there was ever any version of the NIT that gathered from the operating system the IP address of that activating computer.

A. I still need you to be more specific. When you say "gathered" do you mean sent back to the government?

Q. No, I mean gathered.

A. If it wasn't sent to the government, it wasn't gathered.

Q. Okay. Well, what word can I use to --

A. Well, let me rephrase. Who is gathering it, then?

Q. The FBI, through the NIT.

A. So it is sent to the FBI in your question.

Q. I'm not concerned really -- so let me break it down.

So the NIT you can think of as having two stages, right? Part of what the NIT does is once it gets onto our client's computer, onto the activating computer, it gathers certain information, right -- the MAC address, the host name -- gathers that information and then packages that information and sends it -- as part two, it sends that information that it gathered to the FBI server, correct?

A. That's accurate.

Q. Okay. So I'm not concerned for the purposes of this question with what was sent to the FBI. I want you to focus for purposes of this question on what information was gathered to be packaged on the activating computer.

THE COURT: If it wasn't sent to the FBI, how would he know what was packaged?

MR. GRINDROD: Well, Your Honor, I think he's going to testify that --

THE COURT: All right.

THE WITNESS: I'm familiar with Dr. Soghoian's testimony, and I know where you're going with this, so if you will just allow me to testify I think I can put the issue to rest, if that satisfies.

BY MR. GRINDROD:

Q. Well, are you capable of answering the question?

A. Yes, I am capable of answering the question.

Q. Okay. Can you answer the question?

A. The NIT that you're referring to -- I just want to clarify. Is it the one that was used in the matter at hand?

Q. Yes.

A. Okay. So in some instances, for some of the NITs, in order to collect certain pieces of information such as the MAC address the NIT executes a command that displays the MAC address. It also displays, in some cases, the local IP address of the computer, which is also covered by the NIT search warrant. However, that information is not relevant or important to the FBI. It is not parsed out, and it is not sent to the FBI.

So, to answer your question, the NIT itself does not gather an IP address. It does not gather an IP address from the computer. I think you're discussing a semantic argument, but it does not gather it, because that implies that we collected it and received it.

Q. Okay. I don't know what the right word is -- "gather" obviously isn't it -- but I'm trying to get you to focus on not what was sent to the FBI but what your NIT, the FBI NIT, was designed to collect for packaging.

THE COURT: What information is the NIT designed to obtain?

THE WITNESS: Several pieces of information, Your Honor, but the most important one, the one that identifies the defendant, is his IP address, the one that's assigned to him from his Internet service provider. And, so, when the NIT communicates back to the FBI we can see which IP address that communication is coming from.

BY MR. GRINDROD:

Q. So is it correct that, in fact, at least some versions of the NIT collect, not as in transmitting back to the FBI but packaging --

THE COURT: When you use the word "collect" or anything else we're using what information was derived.

Now you want to -- if they -- I assume that we're worried about the words "collect" and "gather," so why don't we use, "What did you learn from this," "What did you expect to learn from it." I don't mind any of this, other than the fact that we're having a dispute as to the terminology of the utilization of words in this case.

And if we can move it along -- that's why I asked what information did they collect -- did they obtain, I should say, not "collect."

MR. GRINDROD: I'll try, Your Honor. The problem --

THE COURT: I don't know where we're going with it. Are you trying to find out what information was on the computer that they did not use?

MR. GRINDROD: Your Honor, I don't know what Agent Alfin will testify to, but I suspect that -- there's reason to believe that the NIT gathered certain information from our clients' computers without transmitting that information back to the FBI and instead deleted or blocked certain aspects of that code from transmitting data and instead transmitted other data through this --

THE COURT: What you're saying, in essence, is you have some information that the FBI has transmitted false information back and claimed it was your defendants' information. Isn't that correct?

MR. GRINDROD: I'm not sure I can make that representation, no, Your Honor.

THE COURT: Well, somewhere or another you're going to have to have some evidence of some kind to go into this. We're all in suppositions, and suppositions are wonderful. In fact, I suppose I'd like to go to the moon, but I don't know if I'm going to get there or live that long. But some people may get there; I'm not sure who. Right now I don't know, but it is possible. Do you understand?

So we're not interested in possibilities, we're interested in, you know, what has happened in this case --

MR. GRINDROD: That's correct.

THE COURT: -- and what the FBI did or did not do.

Now, I understand nothing was encrypted in this case, so consequently the question then is how reliable is it? It appears to me that it may be a jury question as to how reliable something may be, but it is not a legal question of how reliable it is.

MR. GRINDROD: That's true, Your Honor.

THE COURT: So the question really boils down to a question of fact for a jury to determine, unless there is some evidence which would place it in a position where the motion should be granted or not granted here. And so far all I've heard is some suppositions about what's possible on the computer or what can or may be done with computers that are not encrypted.

In fact, I'm not so sure that encryption does much good when I realize how much is stolen from banks over a computer system that's totally encrypted. And I'm only relying on news broadcasts for that; I don't know. I haven't had a case on the stealing from banks by computers.

So the case which we're interested in is was there an unreasonable search in this case resulting in the obtaining of evidence illegally, not a question of whether they legally obtained evidence, so I want to get to that, if I can. And we've been here a couple of hours dealing in the possibilities of various things, and I don't mind going into it, but some of it is farfetched.

MR. GRINDROD: Your Honor is exactly right. I think a lot of these things are questions for the jury.

The reason I'm offering this testimony and a lot of the testimony from Dr. Soghoian was to make clear that there are substantial factual questions, and those questions --

THE COURT: There are always factual questions in that regard. There may be a very simple answer to a lot of simple questions. I'm not in any way suggesting that it's substantial or insubstantial.

MR. GRINDROD: Fair enough, Your Honor.

THE COURT: I make sure that there's no ruling of mine which indicates that possibilities are substantial or insubstantial. Possibilities can grow into more than just possibilities, they can become probabilities, which is a situation that is more than 50 percent of the time.

MR. GRINDROD: I only mean to say, Your Honor, these questions are aimed at our motion to compel, and so that's why some of these may seem like trial issues.

THE COURT: In relation to the motion to compel, there must be some evidence, one, that either the FBI was dishonest or that they wrongly used some search warrant or that the search warrant -- well, in the motion to -- it's not the motion to suppress that deals with the search warrant, we're talking about the motion to compel the disclosure of the code, and I'm not about to disclose the code unless I find that it is material to the defense in this case.

So far I don't know what it is that's been testified to as to the materiality of the code in this case. The question of its materiality has to do with the guilt or innocence of the defendants, and that has to do with did the defendants in this case utilize and receive pornographic material in relation to children, and what the type of the particular material was that it may or may not have received. So far I haven't heard any evidence on materiality in relation to the code. The code merely gave the FBI the means to find the particular Internet company that was delivering material as well as the particular Internet company that received the material. And the question in this case is in discovery it deals with materiality, and we're dealing in a lot of suppositions, Mr. Grindrod.

I'm not trying to chide you or disturb you. There's no question in my mind that the Internet is possible for hackers to do most everything with the Internet. They can even claim to hack the Secretary of State's Internet. Now we know that there's going to be no prosecution of the Secretary of State, so we can talk about it.

But the question is we know that that can be hacked. What is it that we don't know? What we don't know only is what is that code and how valuable is that code, and what could we sell it for, and what could we achieve with it.

I imagine people would pay millions to get that code, enough so that the government wouldn't prosecute some people if I ordered it produced, and they may not prosecute these two if I ordered it produced. But that's only if I find that the material is such as to affect the outcome of this case in some fashion, and I haven't seen it yet.

MR. GRINDROD: I understand, Your Honor. I'll try to --

THE COURT: I'm not trying to stop you.

MR. GRINDROD: Okay.

THE COURT: You've got the fact that, number one, the testimony of the expert is clear. There's no question that there's no protection for that which is transmitted on the Internet. Whatever you transmit on the Internet, somebody can receive it. If it's encrypted, then a clever hacker who can understand how to encrypt things can find it. In fact, the FBI was particularly adept at hacking itself. It hacked into Tor, whether anybody believes it or not. So they hacked in, and they found it, and the question is what did they find? They found a place that transmits child pornography.

I don't know where we're going with child pornography, but it's a very basic thing that we should try to eliminate, if possible; that is, the utilization of children in these matters. In almost every case that I have seen the children of the individuals who utilized them to make these pictures end up with huge problems later on in life -- huge. Or evidently they do. Almost every psychiatrist indicates the same. So the question is whether we can stop the utilization of these children.

MR. GRINDROD: Well, I --

THE COURT: The question before me today is materiality. You know that, I know that.

MR. GRINDROD: And I only have two more quick lines of questioning on those points, Your Honor.

THE COURT: I'm not trying to stop you, I'm trying to define what I'm interested in hearing; not learning about the computer as much as I am about what is material that may help the defendant's case as a matter of probabilities, not possibilities, okay?

MR. GRINDROD: Yes, sir.

BY MR. GRINDROD:

Q. Agent Alfin, how many computers did the NIT deploy against?

A. In the matter at hand for two defendants? Two computers.

Q. For the Playpen operation as a whole, for all users of the Playpen site.

A. There were a number of other defendants who were not charged in the matter at hand. The total number of users that were identified by the FBI is known to me. I would ask the Court's permission not to answer that question, because it could give other individuals insight into the full scope of the FBI's operation.

Specifically, we identified a number of people in foreign countries, and some foreign countries are very slow to act on the information that they receive because it has to go through official diplomatic channels. More importantly, it's not relevant to the matter at hand. In the matter at hand there are two defendants. We deployed the NIT against two computers. Both of those computers are available to the defense. It has no bearing on these defendants how many other people were identified in the case.

THE COURT: But many people were identified, correct?

THE WITNESS: Yes, Your Honor.

MR. GRINDROD: Your Honor, I do think, especially with respect to the particularity argument on our pending motion to suppress, it is relevant. I'm not sure that the legal argument from Agent Alfin is --

THE COURT: I don't know that -- my view is that what they're saying is that it's unique to the proper...

(There was a pause in the proceedings.)

THE COURT: I'm going to sustain the objection made by the witness.

BY MR. GRINDROD:

Q. Is the NIT classified?

A. The NIT is not classified.

Q. Is the exploit?

A. At the moment I believe that it is undergoing review; however, further information about that is answered in the declaration that I believe is under seal.

Q. You testified in a case called United States v. Michaud. Is that correct?

A. I did.

Q. Was the exploit -- well, first of all, was it classified at that time?

A. The actual exploit at that time? I do not believe it was classified.

Q. Was it undergoing review, as you say it is now?

A. I don't know exactly when that review process began. I'm not involved in it.

Q. When did you learn about it?

A. At some point in the past year.

Q. Can you be any more specific?

A. No. Again, the government's position is that the exploit is not material to the case at hand. I don't recall that particular conversation.

However, I did learn in the past year that it is undergoing --

THE COURT: Well, he asked you if it was very material in this case, but the question of determining the exploit, which is the code, I'm not allowing at this time.

MR. GRINDROD: Understood, Your Honor.

BY MR. GRINDROD:

Q. Was the exploit in this case transmitted to everyone against whom the NIT was deployed?

THE COURT: It wasn't transmitted to anyone, as far as I know. Has the exploit itself, the code, been transmitted to anyone, or --

THE WITNESS: Your Honor, if I can clarify some earlier points, there are two important pieces of computer software. The first one is the exploit, and that can be thought of as an open window. So we want to seize information from the defendant's computer, and so there's a vulnerability, an open window, on the defendant's computer. We know about it, and that's how we're able to retrieve information from his computer. So we go in through that open window, the exploit, and then the NIT is the code that we've turned over. That is what seizes the information and sends it back to the government.

So the exploit, the open window, is the part that we have asserted law enforcement privilege. The NIT, the part that actually seizes the data that actually collects information that was used to identify the defendant, that was turned over to the defense in its entirety.

THE COURT: Okay.

BY MR. GRINDROD:

Q. So in your declaration you referred to the exploit as a -- like a defect in the lock of an activating computer.

A. I did.

Q. And you note that what the exploit does is it essentially would allow someone with the proper tool to pick that lock, correct?

A. I don't know if I said "pick lock" -- I may have -- but bypass the lock, yes, that's accurate.

Q. Okay. And, so, in this case for each of our clients the exploit was sent to our clients' activating computer.

A. It was downloaded to their computer, yes.

Q. It was sent from the FBI to their computer physically, correct?

A. They downloaded it from the government's computer, yes.

Q. And, indeed, the exploit was sent every time that the NIT was deployed, correct?

A. The NIT was only deployed once per user in the matter at hand, so "every time" would be once.

Q. Agent Alfin, you just testified a moment ago that the NIT was deployed a large number of times, although you didn't want to specify the precise number.

THE COURT: There's probably many times when he's talking about the hundreds of people that they participated in.

MR. GRINDROD: That's correct.

BY MR. GRINDROD:

Q. And, so, what I'm asking you about, Agent Alfin, is all of these people, not just our clients in this case, but in the whole Playpen operation.

THE COURT: How is that relevant?

MR. GRINDROD: Well, Your Honor, the government is now claiming that the exploit is so sensitive that it can't be turned over. Even with a strong protective order, it can't be reviewed by an identified expert in a safe environment, even at FBI Headquarters, right? And now I believe Agent Alfin will testify that this same code that is so sensitive it can't be disclosed under strict controls was sent out, I don't know, a hundred thousand times or so and could have been recorded in transit.

THE COURT: I don't know about a hundred thousand times, but --

MR. GRINDROD: Well, without them limiting the number down, Your Honor, I think the Court has to assume --

THE COURT: A number of times, and what you're saying is that since the people who received it can discover the code --

MR. GRINDROD: Not discover it, Your Honor, it was sent to them.

THE COURT: It was sent there, but can they determine what the code was that they used to pick the lock?

MR. GRINDROD: Yes, Your Honor.

THE COURT: I don't know. Ask him. Can they?

BY MR. GRINDROD:

Q. Someone recording --

THE COURT: If you use the exploit to go on my computer to determine information, can I know what that code is that you utilized by looking at my computer?

THE WITNESS: The specific answer to that question, Your Honor, is contained in the document that the government has asserted is law-enforcement-sensitive. However, speaking generally, there are a number of pieces of software that can be used so that even if you do send an exploit to someone's computer, even if they know it's happening, even if they try to record it, there are certain pieces of software that could prevent people from doing it successfully.

I'm not authorized to answer whether or not such software was used in this case or how it would have been used; however, the statement that if it is sent to your computer you can see it and analyze it, that on its own is not always accurate.

THE COURT: Well, I'm going to recognize now the law enforcement privilege until I find out if there's any materiality to it, and I'll look at that based on the rest of the evidence that I hear in this case.

MR. GRINDROD: I understand, Your Honor. Just for the record, I would note an objection to that.

THE COURT: I note your objection.

BY MR. GRINDROD:

Q. Agent Alfin, to your knowledge, did any of the people to whom the government sent the exploit that now may or may not be classified -- did any of those people have security clearances?

THE COURT: Does that make any difference?

MS. YUSI: Objection, Your Honor; relevance.

THE COURT: Do you think somebody important may have been on the Internet and wasn't prosecuted? Is that what the question is? I hope it's political.

MR. GRINDROD: The government is claiming that this information is now retroactively classified. They sent it to thousands of people before, and I want to know whether they made any effort to determine whether those people were authorized to handle classified information. I guess it wasn't marked "Classified" at the time, but --

THE WITNESS: The source code that you are seeking in discovery was not sent to anyone.

BY MR. GRINDROD:

Q. Was the exploit sent?

A. Obviously, the exploit was.

Q. Okay. And there was no effort made on the FBI's part to determine whether the people receiving the exploit had some sort of security clearance or were going to handle the exploit properly.

A. As the Court is aware, the users of the Playpen Web site were not known to us before they were identified by the NIT, so we did not know whether or not someone that we were attempting to identify had a security clearance.

MR. GRINDROD: No further questions, Your Honor.

THE COURT: Thank you.

MS. YUSI: Just very briefly.

THE COURT: You don't have to be brief, but --

MS. YUSI: Just to follow up.

REDIRECT EXAMINATION

BY MS. YUSI:

Q. The exploit was sent, but that's not the source code, correct?

A. Correct.

Q. The source code is what the defense is requesting, correct?

A. Correct.

Q. Okay. Just to clarify something that Dr. Soghoian had talked about and the Judge brought up about the IP addresses being different on the PCAP report --

A. Dr. Soghoian testified that the data received by the government was changed in transit.

THE COURT: That's what he said.

THE WITNESS: This is inaccurate and misleading. The actual data --

THE COURT: He said the IPs were changed, as I recall. Go ahead.

THE WITNESS: Again, that statement is misleading. So the IP address that was used to identify the defendant did not change. That, in my declaration, as it states, was not changed in transit. So my declaration -- I believe it was paragraph 19 -- is, again, true and accurate.

What Dr. Soghoian is referring to is the IP address of the government server that is visible in the data that we turned over. He suggests that because that IP address is not a public IP address that it had to change through multiple government servers. That statement is based on an assumption of how the government servers are configured. It is not supported by any testimony in the record or any evidence that the FBI or defense has put in.

A computer can have multiple IP addresses on it, both public and private, the distinction being a public IP address is used to communicate over the Internet. It is the one that was used to identify both of the defendants in the matter at hand. The actual network capture on the government's end occurred on a private IP address on a server connected to the Internet which also had a public IP address. The data that was turned over represents the government's private IP address.

Again, the important thing is that the actual data from the defendant's computers did not change in transit, nor did Dr. Soghoian allege that it did change in transit.

THE COURT: Am I to understand that the computer that sent the material to the government was a different computer than the Playpen computer?

THE WITNESS: So the government ran the Playpen Web site.

THE COURT: Correct.

THE WITNESS: The defendant connected to our Web site --

THE COURT: Correct.

THE WITNESS: -- in the Eastern District of Virginia. He downloaded the NIT and the exploit to his computer.

THE COURT: Right.

THE WITNESS: And then the NIT sent that information back to another government computer. It was not the same computer that had the Web site on it.

BY MS. YUSI:

Q. And that's how it was designed, is that the NIT would send the information to this third computer to -- as a repository?

MR. GRINDROD: Objection, Your Honor; leading.

THE COURT: Objection sustained.

THE WITNESS: So that was how the operation was designed. A user connects to the Playpen Web site, they download the NIT from the Eastern District of Virginia, and then the NIT sends the information back to another government-controlled computer in the Eastern District of Virginia.

THE COURT: So that computer would have been different from the number -- the identification number would have been different from the identification number for the Playpen computer?

THE WITNESS: The actual Playpen Web site was not relevant to the investigation. That was just where we hosted the Web site, and we hosted it within the Tor network. So the IP address of the Playpen server could not be publicly seen, and it's not part of any of the information that's been discussed today.

THE COURT: Well, what were the two IP identifications that were utilized in the correspondence, or the e-mails, or whatever it was that was transmitted?

THE WITNESS: One of them was the defendant's computer --

THE COURT: Yes.

THE WITNESS: -- and the other one was the government's computer.

And so the network data stream that we can see that has been turned over to defense, you can see that entire communication, which includes the information that the government was authorized to collect.

THE COURT: All right. But when Mr. -- I don't quite know how to pronounce his name, Soghoian -- when he testified, he indicated that there was a difference between the number of the IP number and what the government sent. There were two different numbers. Or did he?

THE WITNESS: What Dr. Soghoian suggested was that the data came back to the government computer --

THE COURT: Yes.

THE WITNESS: -- and then went to another government computer.

THE COURT: Correct.

THE WITNESS: That is based on an assumption. That is based on an assumption based on nothing that the government has put in the record, and it is not supported by any evidence that the defense has put on, either.

THE COURT: Well, how did the two IP numbers get involved that he was speaking of?

THE WITNESS: So the NIT transmitted data back to the government.

THE COURT: Yes.

THE WITNESS: And when it did that we could see the defendant's IP address. The NIT knew where to send the information, the government's IP address, because that information is included in the NIT. And, so, the NIT knows where to send the data to because it's included in that package. And, so, it has with it the government's IP address, so it knows where to initiate that connection to. And, so, that is the data that is collected by the NIT, is what can be seen in the evidence that has been turned over.

BY MS. YUSI:

Q. And, just to clarify, Dr. Soghoian talked about headers, correct?

A. Yes.

Q. And did any of the information change? What was he referring to that changed?

A. When Dr. Soghoian suggested that the PCAP data changed, he was referring -- again, the PCAP data has a private government IP address on it, not the public IP address, and so that can be thought of as sending a package through UPS. When it goes through a mail delivery facility, a sorting facility, they slap another sticker on it, it goes where it needs to go, but the package is never opened. It's not ripped open and tampered with, in general.

And, again, as I described previously, we had a number of precautions in place to prevent such tampering. However, the important thing is that the data that was sent from the defendant's computer was done so accurately, and we captured it accurately.

Q. And Dr. Soghoian agrees that nothing had changed in the data.

A. Dr. Soghoian agrees that there was no evidence that any of the data was tampered with, is my recollection.

MS. YUSI: That 's all of my follow-up, Your Honor.

MR. GRINDROD: Your Honor, may I briefly address those points with the witness?

THE COURT: Is it something new?

MR. GRINDROD: No, Your Honor. Well, it is limited to points that were directly raised about what our expert's testimony was and whether it should be credited, two quick lines of questioning, Your Honor.

THE COURT: You've got two questions.

RECROSS-EXAMINATION

BY MR. GRINDROD:

Q. You just testified that when Dr. Soghoian said that, based on his observations of the PCAP data, it looked like the information that was sent back to the NIT went to a public government IP address and then went to another government computer, right? And you said that was speculation; there was no evidence in the record of that, right?

A. That's not an accurate quote, and the question doesn't make sense from a technical standpoint. Can you restate it, please?

Q. Sure. So you talked about Dr. Soghoian's testimony and how he said that by looking at the PCAP data it was his opinion that the information that was sent from our clients' computer to -- was sent initially to an FBI server and then to some other FBI server, and that he could tell that because the PCAP data indicated that the IP address was associated with this second private server, nonpublic government server, remember?

A. Yes, that is what he testified to.

Q. And you said that was speculation and there was no evidence in the record to support it, correct?

A. I did.

Q. But that is, in fact, what happened, right?

A. No. As I stated, a server can have more than one IP address on it. So just because the IP address changes doesn't mean it went to another server.

Q. Okay. So in this case the IP address changed. You agree with that?

A. Which IP address?

Q. The IP address that's reflective of the government's receipt of the information in the NIT.

THE COURT: Let's get a specific -- you know, I get lost. I try to understand everything. So far I'm not sure what IP address we're speaking of that changed.

There was an IP address, according to the expert, the good doctor, that the numbers were different, okay? Not the data was different, the numbers were different, the IP numbers.

MR. GRINDROD: Right.

THE COURT: But I'm not sure it was material that was transmitted to the FBI, so I don't know where it was transmitted from or to whom it was transmitted. And we have so many computers in this case I'm beginning to get confused about the computers.

He indicated, the expert did, that there was a computer that received the information; that is, it went into the defendant's computer, got certain information, transferred it to a government computer, which then transferred it to another government computer, which transferred it to the FBI. Is that what you understand his testimony to be, or am I wrong?

MR. GRINDROD: I think there may be one extra computer in there, Your Honor, but that is essentially --

THE COURT: Well, tell me what you understood it to be so I can be on the safe side.

They obtained it from the defendant's computer.

MR. GRINDROD: That's correct.

THE COURT: And then it went to where?

MR. GRINDROD: It was routed through our clients' wireless router, not directly but eventually went to an FBI -- a government computer, and then, after that point, went to either -- went -- there were some further transfers, and between when it went to the FBI initially and when it was subsequently transferred there was a change in the IP address, of the receiving IP address, as displayed in the PCAP data.

THE COURT: It wasn't the defendants' IP address.

MR. GRINDROD: Not that I was talking about there, Your Honor. There's a separate issue as to whether the IP address that --

THE COURT: The IP address that we're speaking of was the government's IP address, correct?

MR. GRINDROD: In that instance, yes, Your Honor.

THE COURT: Okay. I just want to make sure. Everything else there's been no contest over. We're in a contest about what was received was a different IP address for the government.

MR. GRINDROD: Well, and for our clients, Your Honor, but that's for a slightly different reason. Well, a very similar reason but based on --

THE COURT: I thought it was in the receipt of the information that the FBI had --

MR. GRINDROD: It's both, Your Honor.

THE COURT: -- and it received it from a government computer someplace.

MR. GRINDROD: Yes, that's correct, Your Honor.

THE COURT: And when they received it I understand that we had an IP address that was different from some government IP address, correct?

MR. GRINDROD: Yes, Your Honor.

THE COURT: Okay. It was not the difference of the defendants' IP address.

MR. GRINDROD: It was that, also, Your Honor.

THE COURT: I never heard him testify about the defendants' IP address. He's still here, so I'll ask him about it.

Okay, that's it. Let's go. I'm pretty sure he said it was the government's IP address.

MR. GRINDROD: Well, I think, Your Honor, that he testified --

THE COURT: I don't want to "think" anymore.

MR. GRINDROD: Okay.

THE COURT: I'll find out what he said.

BY MR. GRINDROD:

Q. Let me ask you this question, Dr. Alfin:

So you made this distinction between the information that was inside the package and the information that may be displayed on the outside of the package, right?

A. There is a distinction. And, for the record, I just want to be clear. I am not a doctor.

Q. So, Agent Alfin.

A. I just wanted to make sure I'm not --

THE COURT: We're not going back over all the testimony. No more.

You've got one more question. You said you had two. I've allowed you plenty. You have one more question, and that's it. Make sure it's a good question.

BY MR. GRINDROD:

Q. Even though you make this distinction between the information that's in the package not changing, whereas, perhaps the information on the outside did, in fact, the information that allowed you to find my client was the information on the outside of the package, correct?

A. The information that allowed us to identify your client never changed.

Q. That's not what I asked you.

A. It was on the outside of the package, but it never changed.

Q. Thank you.

MR. GRINDROD: No further questions, Your Honor.

THE COURT: Anything else from this witness?

MS. YUSI: Not from the government, Your Honor.

MR. GRINDROD: Not from the defense.

THE COURT: Thank you very much, sir. You may step down.

THE WITNESS: Thank you, Your Honor.

THE COURT: Do you want to recall your witness, sir?

(There was a pause in the proceedings.)

MR. GRINDROD: I will briefly, Your Honor, just to address that one point that we were talking about.

THE COURT: All right, I'm going to allow you to.

MR. GRINDROD: Your Honor, the defense recalls

Dr. Soghoian.

THE COURT: You're reminded you're still under oath.

CHRISTOPHER SOGHOIAN, Ph.D., recalled as a witness, having been first duly sworn, testified as follows:

DIRECT EXAMINATION

BY MR. GRINDROD:

Q. Dr. Soghoian, were you present for the last exchange with Agent Alfin?

A. I was.

Q. And there was some question as to which IP address we were talking about, whether it was the government IP address or our clients' IP addresses. Do you remember that?

A. I do.

Q. Can you explain to the Judge what, if any, IP address changed?

A. Yes, Your Honor. There were two IP addresses that are displayed in the PCAP file; the IP address of the computer that ran the NIT, the defendants' computers, and then there's an IP address for the government.

What I believe is that the IP address -- that both IP addresses, in fact, changed between when the data left the computer of the defendant and when the data was received ultimately by the final government server.

THE COURT: All right. Now, it's very simple. There has to be some documentation that you reviewed that saw it. Where is that documentation?

THE WITNESS: So the government has provided us a copy of the -- or provided counsel, who then provided me, a copy of the PCAP file, which is the recording, and when I looked at the PCAP file --

THE COURT: Well, let me have the PCAP file. I want the PCAP file now.

THE WITNESS: The PCAP file is not in a form that is easy for the -- for someone not skilled in the art to understand. After this hearing, when I get back to their office, I can provide a screenshot --

THE COURT: I don't want you to provide anything when you get back to the office. I want to see the PCAP thing now. I can employ an expert, don't worry.

Let me have the PCAP file right this minute. Somebody's got it, the one that was shown to Mr. -- this expert witness.

It's on a disk? There wasn't anything -- nothing printed out?

MR. GRINDROD: This is exactly as we received it from the government, Your Honor.

THE COURT: Is this what you reviewed?

THE WITNESS: Counsel e-mailed me a copy of the files that were encrypted. I decrypted those files. I believe the encryption was performed by the government.

THE COURT: Let me see what you e-mailed to the witness.

MR. GRINDROD: It's the files that are contained on this disk, Your Honor. I didn't --

THE COURT: Well, where is the copy of it?

MR. GRINDROD: Your Honor, I don't have a copy in any other form than on this disk.

THE COURT: You don't keep copies of what you send to people?

MR. GRINDROD: Well, Your Honor, it's --

THE COURT: You don't keep copies of what you send in your mail?

MR. GRINDROD: It was -- it was -- I don't have any other copy of this.

THE COURT: I didn't ask you about the copy of this. What did you send to this witness? It wasn't that.

MR. GRINDROD: Your Honor, I dragged the files from this disk into an e-mail, I sent that to Dr. Soghoian, I sent, through separate means, an encryption code, and --

THE COURT: You sent an e-mail to him.

MR. GRINDROD: That's correct, Your Honor.

THE COURT: Okay. And you don't have a copy of the e-mail?

MR. GRINDROD: Not with me, no, Your Honor.

THE COURT: I know you don't have it with you. The computer isn't here.

MR. GRINDROD: That's correct.

THE COURT: So you have a copy. Tomorrow morning get that copy to me.

MR. GRINDROD: Yes, Your Honor.

THE COURT: Now, that's a copy furnished to you by the government?

MR. GRINDROD: That's correct, Your Honor.

THE COURT: And who encrypted it?

MR. GRINDROD: The government, Your Honor.

THE COURT: Oh, so the government gave you a copy.

Do you have a copy of what you gave him, Ms. Yusi?

MS. YUSI: Your Honor, I did not bring it. It's actually a program file, I understand, and so it's not something that you just -- it doesn't come up in a Word document that you can print out. You actually have to look at it along with other technology in order for it to appear as anything.

THE COURT: Well, forget it. It's getting too complex now.

So the only way you can determine it is to look at it with other technology.

MS. YUSI: That's my understanding.

THE COURT: Okay. But you sent him an e-mail, correct?

MR. GRINDROD: Yes, Your Honor, containing the file.

THE COURT: Are you sure somebody didn't hack your e-mail on the way?

MR. GRINDROD: Well, we used encryption, Your Honor.

THE COURT: Oh, you used an encrypted e-mail?

MR. GRINDROD: Yes, Your Honor.

THE COURT: Oh, that's excellent.

Okay. We'll see where we're going. I'm still worried about the materiality, but I am concerned about the fact that IP addresses were changed. I'm curious about what that is.

And I'm going to request you to see if you can't copy the e-mail and send it to me. I'm asking the government to send me a copy of the encryption of this concerning the IP addresses.

MR. GRINDROD: And, Your Honor, if it also would be helpful -- I know the Court wants the data itself, but Dr. Soghoian showed me the data --

THE COURT: I don't want to hear from Dr. Soghoian any more.

MR. GRINDROD: Not -- just --

THE COURT: That's it. He's testified. That's it.

MR. GRINDROD: Just the raw data.

THE COURT: I just want to see what's on the encryption.

MR. GRINDROD: Will do, Your Honor.

THE COURT: I mean, whatever was encrypted. I want to see the e-mail, the various -- the original document and what the government says it gave to the defendant in relation to some encryption, okay?

Anything else?

MR. GRINDROD: No, Your Honor.

THE COURT: Anything else, ma'am?

MS. YUSI: A follow-up, Your Honor.

CROSS EXAMINATION

BY MS. YUSI:

Q. The defendant's IP address that was sent in the package to the FBI server --

A. That was received, you mean?

Q. That was received, yes, sent by his computer through the NIT. The NIT sent it, correct?

A. The PCAP shows it was received, and if you're going to ask me about the IP address, that changed along the way.

Q. Okay. But that's the IP address that Cox or the local ISP -- went to the defendant's residence. Is that right?

A. Are you asking me if that's what is in the PCAP file or if that's what left the defendants' computer?

Q. What's in the PCAP file contains an IP address that led to the defendants, correct?

A. I believe so.

Q. Thank you.

MR. GRINDROD: I have nothing further, Your Honor.

THE COURT: I don't have anything further. Thank you very much. You may step down, sir.

All right. Tomorrow I want those furnished to me, by 12:00 noon tomorrow, that e-mail you sent, the encryption that you gave them, whatever that encryption was, and a copy of this thing that was given to the government. I'm more interested in the change in the IP address than anything else.

In relation to the materiality, is there any other evidence concerning the materiality, to the defense, of the code?

(There was a pause in the proceedings.)

MR. GRINDROD: Nothing further from the defense, Your Honor.

THE COURT: Anything else, Ms. Yusi?

MS. YUSI: Not from the government.

THE COURT: Insofar as the motion to suppress is concerned, that is denied at this time. I will forward an opinion. It will probably take maybe a couple of weeks to get the opinion out.

As well, I'm going to look at this question of the materiality of the information of the code. I'm having lots of problems finding any materiality, but I want to look through all of these -- I have not read the testimony that was filed given in Judge Morgan's court, except that I did not necessarily agree with everything in his decision. Although, I found it a brilliant decision and a great law review article; however, I must say -- and I mean that sincerely. It thoroughly investigated the law.

Insofar as the materiality is concerned, I want to look at what's testified to there, and then I can probably give you a decision. I'll try to give you a decision, but I can't get a written out because it's somewhat complex, and I figure it will take a couple of weeks to get the opinion out. It's not the only case I have.

Anything else?

MS. YUSI: Not from the government. Thank you, Your Honor.

THE COURT: Now, the question is do you want to take some time to argue this matter tomorrow morning?

MS. YUSI: Your Honor, I don't have anything to add that the Court hasn't heard at this point.

THE COURT: Do you want to argue the matter tomorrow, Mr. Grindrod or Mr. Cejas or Mr. Colgan?

MR. GRINDROD: Your Honor, unless -- I mean, we'd be happy to address any concerns the Court has, but --

THE COURT: I'm not trying to -- I'm just giving you the opportunity if you want to.

MR. GRINDROD: I appreciate it, Your Honor.

THE COURT: Okay. Thank you very much.

(The hearing adjourned at 6:02 p.m.)

CERTIFICATION

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s

Heidi L. Jeffreys

July 14, 2016

Date